ITI LTD

RFP (NIT)
Selection of an Experienced IT-Networking Partner
For
IT Infrastructure Implementation for ERP and other
Future Digital Initiatives at NMDC Locations.

Ref: CRP20E001; Date: 20/05/2020

This RFP contains 54 Pages

Ref: CRP20E001   Date:20/05/2020

ITI Limited, a Government of India Undertaking invites sealed priced bid proposals under single stage bidding and two stage bid opening, using Two Electronic Envelope System through the e-Tendering process, from Experienced and Capable IT-Networking Supply & Implementation Companies for and on behalf of NMDC (National Mineral Development Corporation) for the following scope of work on turn key basis.

	Date	Time
Last date for Clarification	27/05/2020	IST 17:00 HRS
Uploading of Corrigendum:	29/05/2020	IST 17:00 HRS.
Due Date for Submission of RFP is	11/06/2020	IST 12.00 HRS.
Opening of Technical Bid	11/06/2020	IST 15:00 HRS.

1.	**Scope of Work:**
(a).	Establishment of a DC and DR (on Co-Location basis at MeitY Empaneled Service Providers) to host the Applications of NMDC such as SAP S/4 HANA ERP at DC, located in Hyderabad and DR located in another city and another seismic zone.
(b).	Supply, Installation, Integration, Testing, Commissioning and Support (SiitcS) of LAN and WAN Networks.
(c).	Provide/ Upgrade of existing MPLS/ VPN at 15 locations.
(d).	To submit a detailed design and deployment methodology and implementation plan of execution of the project.
(e).	Integrate and upgrade Internet leased lines at HO, Projects and other locations.
(f).	Deployment of secured security solutions.
(g).	Provision of secured encrypted VPN over the internet for remote access to applications.
(h).	Inter Connecting the nodes with Optical fiber or Radio links, including Supply, Installation, Integration, Testing, Commissioning and maintenance Support (SiitcS).
(i).	SiitcS of Wi-Fi zones (Indoor/outdoor) at HO, Projects and other locations, to cater to data needs of current and future requirements of NMDC.
(j).	Various Services, connected with the project.
(k).	Managed Services.
	Note 1: The detailed scope of work, Technical Specs and BoQ available with the main document. *Note 2: 5 Years Comprehensive Warranty and maintenance support needs to be provided to all the elements of network.*

2.		**Eligibility Criteria**
(i).		The bidder must be, a company registered in India, under the companies Act – 1956 or 2013 and should be in business of IT /ITES/ Networking for at least 5 years.
(ii).		Average Annual financial turnover during the last 3 years, ending 31st March-2019 should be at least Rs. 100 Cr. Audited financial statements for the last 3 years (2016-17, 2017-18, 2018-19) to be enclosed.
(iii).		The bidder should be financially strong having Positive Net worth in each of the last 3 financial years.
(iv).		The intending bidder must be an IT/ITES/Networking company, having an Experience of successfully executing similar nature of works as mentioned in the Scope of Work viz. setting up of DC/DR (H/w & S/w), Firewalls, active Switches, Managed Services, Backbone cabling, Setting up of Wi-Fi Networks, laying of WAN/LAN Networks and laying of OFC etc. during the last 7 years (as on 31st March'2020) of at least following value/billing: **One Project costing Rs 80 Cr OR Two projects costing Rs 50 Cr. each OR Three Projects costing Rs 40 Cr. each**.
		The project/projects claimed towards experience, must contain one or more elements essentially from each of the following three categories. Elements of Category (a) below, must contribute at least 30% cost of the project.
	(a)	The establishment of DC/DR, Fire-walls and Managed services.
	(b)	Active Switches, EMS and Backbone Cabling with associated IT components.
	(c)	Wi-Fi, P2P radio links and Laying of Underground OFC Networks.
(v).		IT Service & Security Accreditations: The intending bidder must possess the following certifications on the date of submission of the bids:
	(a).	Valid ISO 20000 Certificate
	(b)	Valid ISO 27000 Certificate
	(c)	Valid CMMi Level 3 or above, certificate
(vi).		The bidder should have MAF from respective OEM(s) for addressing this RFP, which the bidder proposes to use in this project.
(vii).		Authorization letters from OEM's concerned (MAF) to address this business opportunity needs to be enclosed in the given format. Bids without authorization will not be considered.
(viii).		The bidder should not have been black listed by central / state governments / PSUs as on date of bid submission.
(ix).		Bidders need to quote for one of the brands of the equipment identified by the user and mentioned in the technical specs / Bill of Material. No other brand will be considered.

3	**Bid Submission:**
	(i) EMD for Rs. 2.0 Cr. which can be submitted in the form of DD or Bank Guarantee, valid for 6 months. Technical Bids without EMD will not be considered.
	(ii) Validity of bids 90 days from the date of opening of the Bid.
4.	Five years on site comprehensive warranty would be provided by the concerned OEMs, an undertaking confirming the same from the OEMs along with the offer,must.
5.	A PBG of 10% needs to be submitted by the successful bidder for the period of delivery and execution and 5% for 63 Months thereafter.

![ITI logo]	**ITI LIMITED**	**Phone Nos:**	**080-25618291**
			080-25614466 Ext.2263

REGD. & CORPORATE OFFICE, ITI BHAVAN
DOORAVANINAGAR, BENGALURU - 560 016, INDIA
NOTICE INVITING TENDER

	TENDER TYPE:	**Two Bid**
	NIT REFERENCE :	CRP20E001
	NIT DATE:	**20-05-2020**

Please quote your best prices for the item as mentioned below.

SI NO	**ITEM DESCRIPTION**	**Quantity**
1)	**Selection of an Experienced IT-Networking Partner For IT Infrastructure Implementation for ERP and other Future Digital Initiatives at NMDC Locations**	

Note:	1	Offers are to be submitted strictly as per details furnished in this RFP
	2	Bidders have to submit **EMD** as per Clause. No.3 (a) **on or before the 10-06-2020, 17:00 HRS.(IST)**

FOR SUBMISSION OF ONLINE BID AND PROCEDURE TO BE FOLLOWED
VISIT www.tenderwizard.com/ITILIMITED

All vendors have to register in website: www.tenderwizard.com/ITILIMITED for submitting online BID

BID DUE DATE AND TIME:	**11-06-2020**	**12:00 HRS**
BID OPENING DATE AND TIME (ONLY TECHNICAL BID)	**11-06-2020**	**15:00 HRS**

Tender type: Two Bid viz. 1)Technical Bid. 2)Price Bid.	For ITI Limited Dy. General Manager-MM & CPIO Ph: 080-25618291(Direct), 080-25614466 Extn:2263 Email: lokeshpn_crp@itiltd.co.in

C O N T E N T S

ITI Limited
Regd. & Corporate Office
ITI Bhavan, Dooravaninagar,
BANGALORE – 560016
CIN No: L32202KA1950GoI000640

Ref: CRP20E001   **Date: 20/05/2020**

ITI Limited, a Government of India Undertaking invites sealed priced bid proposals under single stage bidding and two stage bid opening, using Two Electronic Envelope System through the e-Tendering process, from Experienced and Capable IT-Networking Supply & Implementation Companies for and on behalf of NMDC (National Mineral Development Corporation) for the following scope of work on turn key basis.

Due Date for Submission of RFP is 11/06/2020 before 12:00 HRS(IST).

1.		**Scope of Work**
	a.	Establishment of a DC (Data Centre) and DR (Disaster Recovery Centre) (on Co-Location basis at MeitY Empaneled Service Provider) to host the Applications of NMDC such as SAP S/4 HANA ERP at DC, located in Hyderabad and DR located in another city and another seismic zone.
	b.	Supply, Installation, Integration, Testing, Commissioning and Support (SiitcS) of LAN and WAN Networks.
	c.	Provide/ Upgrade existing MPLS/ VPN at 15 locations of NMDC namely: i. NMDC HO, Hyderabad ii. Kirandul Iron Ore Mining Complex, Dantewada, Chhattisgarh iii. Bacheli Iron Ore Mining Complex, Dantewada, Chhattisgarh iv. Donimalai Iron Ore Mining Complex, Bellary, Karnataka v. NISP, Jagdalpur, Chhattisgarh vi. DMP, Panna, Madhya Pradesh vii. R&D Centre, Hyderabad viii. SIU, Paloncha ix. GEC, Raipur x. RO, Visakhapatnam xi. RO, Bhubaneswar xii. RO, New Delhi. xiii. RO, Chennai xiv. RO, Bengaluru xv. RO, Kolkata
	d.	To submit a detailed design and deployment methodology and plan of execution of the project for the approval before its implementation.

	e.	Integrate / upgrade Internet Leased Lines (ILL) at HO, Projects and other locations of NMDC.
	f.	Deployment of secured security solutions.
	g.	Provision of secured encrypted VPN over the internet for remote access to applications.
	h.	Inter Connecting the nodes with Optical fiber or Radio links, including Supply, Installation, Integration, Testing, Commissioning and maintenance Support (SiitcS).
	(**Detailed Scope of work to be referred for compliance, is enclosed at Annexure-I**).	
	Note: 5 Years Comprehensive Warranty and maintenance support needs to be provided to all the elements of network.	
	The required MPLS and ILL connectivity from the TSPs shall be arranged separately and bidder need not to account for its cost.	
	(Technical Specifications are enclosed at **Annexure-II**)	

2.		**Eligibility Criteria**
a.		The bidder must be, a company registered in India, under the companies Act – 1956 or 2013 and should be in business of IT / ITI ES/Networking for at least 5 years.
b.		Average Annual financial turnover during the last 3 years, ending 31st March-2019 should be at least Rs. 100 Cr . Audited financial statements for the last 3 years (2016-17, 2017-18, 2018-19) to be enclosed.
c.		The bidder should be financially strong having Positive Net worth in each of the last 3 financial years.
d.		The intending bidder must be an IT/ITES/Networking company, having an Experience of successfully executing similar nature of works as mentioned in the Scope of Work viz. setting up of DC/DR (H/w & S/w), Firewalls, active Switches, Managed Services, Backbone cabling, Setting up of Wi-Fi Networks, laying of WAN/LAN Networks and laying of OFC etc. during the last 7 years (as on 31st March'2020) of at least following value/billing: **One Project costing Rs 80 Cr OR Two projects costing Rs 50 Cr. each OR Three Projects costing Rs 40 Cr. each**.
		The project/projects claimed towards experience, must contain one or more elements essentially from each of the following three categories. Elements of Category (i) below, must contribute at least 30% cost of the project.
	(i)	The establishment of DC/DR, Fire-walls and Managed services.
	(ii)	Active Switches, EMS and Backbone Cabling with associated IT components.
	(iii)	Wi-Fi, P2P radio links and Laying of Underground OFC Networks.
		(Project-Wise, Work order copies and completion certificates, depicting various project elements and costs thereof, with MAF details, to be enclosed).
e.		IT Service & Security Accreditations: The intending bidder must possess the following certifications on the date of submission of the bids:
	(i).	Valid ISO 20000 Certificate
	(ii)	Valid ISO 27000 Certificate
	(iii)	Valid CMMi Level 3 or above, certificate
f.		The bidder should have MAF from respective OEM(s) for addressing this RFP, which it proposes to use in this project.
g.		Authorization letters from OEM's concerned (MAF) to address this business opportunity needs to be enclosed in the given format. Bids without authorization will not be considered. List of MAF.s required is at **Annexure-XI**I

h.	The bidder should not have been black listed by central / state governments / PSUs as on date of bid submission. Self-certificate shall be submitted in this regard. **(Annexure-X)**
i.	Bidders must quote for one of the brands of the equipment as identified by the user and mentioned in the technical specs / Bill of Material. No other brand will be considered.
j.	The bidder shall submit an undertaking that they do not have any ongoing disputes on statutory levies like Income Tax, GST, PF, ESI etc.
k.	Authorization letter in company letter head authorizing the person signing the Bid for this RFP.
l.	Clause by Clause compliance of RFP terms & conditions needs to be submitted. Non-compliance on technical specifications and offers with deviations are liable to be rejected.

3.	**Bid Submission:**
a.	**EMD for Rs. 2.0 Cr** should be furnished along with the technical Bid. EMD can be in the form of DD in favour of ITI Limited – Bangalore or Bank Guarantee (**as per Annexure -V**) valid for 6 months. Technical Bids without EMD will not be considered. Eligible MSME firms registered with MSME need not furnish EMD. For availing this exemption, certified copy of NSIC/MSME certificate need to be enclosed along with the technical bid
b.	Separately sealed, Technical bid and financial bids to be submitted as explained in this RFP.
c.	Validity of bids 90 days from the date of opening of the Bid.
d.	Documents related to eligibility criteria should be enclosed along with technical bid.
e.	The bidder should quote for all the items in the bill of materials. Bids not quoting for all items will not be considered.
f.	Financial bids of bidders who are not meeting/qualifying the eligibility criteria /technical qualifications will not be opened and will be returned.
g.	Five years on site comprehensive warranty would be provided by the concerned OEMs. An undertaking confirming the same from the OEMs should be enclosed along with the offer.
h.	No criminal case should be pending against the bidder anywhere in India. Self-certification should be provided to this effect
i.	In the event of breach of contract, the entire amount of EMD/Security Deposit shall stand forfeited.
Note:	**Price details should be available only in the price Bid and relevant annexures. If it is available in technical bid or elsewhere, bid will be rejected.**

4. Other Conditions:	
a.	The selected bidder for implementation of the project, **PIP (Project Implementation Partner)** shall submit a detailed design and deployment methodology and implementation plan of execution, soon after LOI, for ITI/NMDC's approval.
b.	PIP shall provide fortnightly physical and financial progress report of the project to ITI.
c.	PIP shall be wholly responsible for the safe keeping, security, protection of assets created etc. at the respective site till the installation of equipment/material and any loss or damage to the assets created shall be indemnified by the PIP.
d.	PIP shall be responsible for ensuring the quality standards of all the equipment, services & works of the project. Accordingly, PIP shall facilitate inspections by ITI / NMDC Personnel to ensure the quality standards and for monitoring progress of the work as may be desired/advised by the ITI/NMDC. PIP shall provide all the information and assistance required to the inspecting/AT team of ITI/NMDC. If during the inspection, any defects or variation are observed the same will have to be rectified by PIP immediately.

e.	The successful bidder (**Project Implementation Partner**) would ensure that all the software upgrades/updates/ Patches and licenses are installed and validity maintained, free of cost throughout the warranty and support period of five years for seamless functioning.
f.	The **Project Implementation Partner** (PIP) needs to comply all EPF and ESI stipulations and guidelines.
g.	**Approach & Methodologies:** (i). The bidder needs to provide Project Strategy, management and relationship with various OEMs for the smooth rollout of the Project and conformity to functional requirements including project time lines. (ii). The bidder needs to indicate it's capabilities along with the details of Internal trainers to conduct onsite and offsite trainings to the team of NMDC engineers and resources deployed by ITI for the Project.

5. Check list of documents/information to be submitted with the bid:	
a.	Company Profile.
b.	Certificate of Incorporation.
c.	Memorandum & Articles of Association.
d.	Audited financial statements for the last 3 years. (2016-17, 2017-18 & 2018-19) and CA certificate.
e.	Certificate from Statutory Auditor/CA specifying the Annual Turnover from ICT services during last three years (2016-19).
f.	Experience Certificates: Work Order / Agreements of the Project along with completion certificates clearly highlighting Scope of the Work (SOW), Bill of Material (BOM), cost of the Project(s) with specific mention of the cost towards DC/DR, Fire-walls and Managed services, project wise. The experience undertaken during the last 7 years only (period ending 31st March 2020), shall be considered.
g.	Net Worth Certificate for the last 3 years (2016-19).
h.	GST Registration Certificate.
i.	Copy of PAN Card.
j.	CIN (Corporate Identity Number).
k.	Copies of ISO Certificates.
l.	Self-declaration in **Annexure-X** non barring from business on account of blacklisting etc.
m.	Authorization letter in the company letterhead authorizing the person signing the bid for this RFP and Power of Attorney (POA).
n.	Clause by clause compliance to all the terms and conditions.
o.	Undertaking in letter head to indemnify ITI from any claims / penalties / statutory charges, liquidated damages, with legal expenses etc.
p.	NDA (Non-Disclosure Agreement) as per **Annexure VIII**.
q.	Letter(s) of Authorization from OEMs allowing to bid, using their Brand of Equipment and post commissioning, onsite support for 5 years (in MAF format provided) as per **Annexure XI**
r.	Pre-Contract Integrity Pact **Annexure –IX**.
s.	A detailed exhibit on the "Approach and Methodology", bidder proposes to adopt if the project is awarded to it.
t.	All other docs as mentioned in this RFP elsewhere. Scope of this RFP matches NMDC technical specifications, installation and acceptance guidelines.

6.	**E-tendering Instructions to Bidders:** Submission of Bids shall be only through online process which is mandatory for this Tender.
6.1	**Tender Bidding Methodology:** **Sealed Bid System** Tender Type: Two bids i.e., Technical and Financial Bids shall be submitted by the bidder at the same time on the portal.
6.2	**Broad outlines of the activities from Bidders prospective:**
6.2.1.	Procure a Digital Signing Certificate (DSC)
6.2.2	Register on Electronic Tendering System® (ETS)
6.2.3	Create Users and assign roles on ETS
6.2.4	View Request for Proposal (RFP) on ETS
6.2.5	Download Official Copy of Tender Documents from ETS
6.2.6	Clarification to Tender Documents on ETS
6.2.7	Query to ITI LTD (Optional)
6.2.8	View response to queries posted by ITI LTD, as an addendum/corrigendum.
6.2.9	Bid Submission on ETS
6.2.10	Attend Public Online Tender Opening Event on ETS Opening of Technical/Financial Part
6.2.11	View Post-TOE Clarification posted by ITI LTD on ETS (Optional) Respond to ITI LTD's Post-TOE queries.
6.3	For participating in this tender online, the following instructions need to be read carefully. These instructions are supplemented with more detailed guidelines on the relevant screens of the ETS. **Note 1**: It is advised that all the documents to be submitted are kept scanned or converted to PDF format in a separate folder on your computer before starting online submission. BOQ (Excel Format) may be downloaded and rates may be filled appropriately. This file may also be saved in a secret folder on your computer. **Note 2:** While uploading the documents, it should be ensured that the file name should be the name of the document itself.
6.4	**Digital Certificates:** For integrity of data and its authenticity/ non-repudiation of electronic records, and be compliant with IT Act 2000, it is necessary for each user to have a Digital Certificate (DC) also referred to as Digital Signature Certificate (DSC), of Class 3 or above, issued by a Certifying Authority (CA) licensed by Controller of Certifying Authorities (CCA) [refer http://www.cca.gov.in]. Checklist for obtaining DSC by International Bidders may be followed.
6.5	**Registration in e-procurement portal:** Bidder has to Register first in https://www.tenderwizard.com/ITILIMITED and then Tender document can be downloaded from the web site: https://www.tenderwizard.com/ITILIMITED and bid has to be submitted in the e-format.
6.6	**ITI LIMITED has decided to use process of e-tendering for inviting this tender and thus the physical copy of the tender would not be sold.**
6.7	**Special Note on Security of Bids:**

	Security related functionality has been rigorously implemented in ETS in a multi-dimensional manner. Starting with 'Acceptance of Registration by the Service Provider', provision for security has been made at various stages in Electronic Tender's software. Specifically, for Bid Submission, some security related aspects are outlined below: - As part of the Electronic Encrypt functionality, the contents of both the 'Electronic Forms' and the 'Main-Bid' are securely encrypted using a Pass-phrase created by the server itself. The Pass phrase is more difficult to break. This method of bid-encryption does not have the security and data-integrity related vulnerabilities which are inherent in e-tendering systems which use Public-Key of the specified officer of a Buyer organization for bid-encryption. Bid-encryption in ETS is such that the Bids cannot be decrypted before the Public Online Tender Opening Event (TOE), even if there is connivance between the concerned tender opening officers of the Buyer organization and the personnel of e-tendering service provider.
6.8	**Public Online Tender Opening Event (TOE):** ETS offers a unique facility for 'Public Online Tender Opening Event (TOE)'. Tender Opening Officers as well as authorized representatives of bidders can attend the Public Online Tender Opening Event (TOE) from the comfort of their offices. For this purpose, representatives of bidders (i.e. Supplier organization) duly authorized are requested to carry a Laptop and Wireless Connectivity to Internet. Every legal requirement for a transparent and secure 'Public Online Tender Opening Event (TOE)' has been implemented on ETS. As soon as a Bid is decrypted with the corresponding 'Pass-Phrase' as submitted online by the bidder himself (during the TOE itself), salient points of the Bids are simultaneously made available for downloading by all participating bidders. The work of taking notes during a manual 'Tender Opening Event' is therefore replaced with this superior and convenient form of 'Public Online Tender Opening Event (TOE)'. ETS has a unique facility of 'Online Comparison Chart' which is dynamically updated as each online bid is opened. The format of the chart is based on inputs provided by the Buyer for each Tender. The information in the Comparison Chart is based on the data submitted by the Bidders in electronic forms. A detailed Technical and/ or Financial Comparison Chart enhance Transparency. Detailed instructions are given on relevant screens. ETS has a unique facility of a detailed report titled 'Minutes of Online Tender Opening Event (TOE)' covering all important activities of 'Online Tender Opening Event (TOE)'. This is available to all participating bidders for 'Viewing/ Downloading'.
6.9	**Other Instructions:** For further instructions, the vendor should visit the home page of the portal https://www.tenderwizard.com/ITILIMITED. **Important Note**: It is strongly recommended that all authorized users of Supplier organizations should thoroughly peruse the information provided under the relevant links, and take appropriate action. This will prevent hiccups, and minimize teething problems during the use of ETS.
6.10	**The following 'FOUR KEY INSTRUCTIONS for BIDDERS' must be assiduously adhered to:**

6.10.1	Obtain individual Digital Signing Certificate (DSC or DC) well in advance of your tender submission deadline on ETS.
6.10.2	Register your organization on ETS well in advance of your tender submission deadline on ETS.
6.10.3	Get your organization's concerned executives trained on ETS well in advance of your tender submission deadline on ETS.
6.10.4	Submit your bids well in advance of tender submission deadline on ETS to avoid any unforeseen last-minute problems due to internet timeout, breakdown, etc. While the first three instructions mentioned above are especially relevant to first-time users of ETS, the fourth instruction is relevant at all times.
6.11	**Minimum Requirements at Bidders end:** Computer System with good configuration and OS preferably supporting Windows Word, Excel & PDF, High Speed Broadband connectivity, Internet Browser and Digital Certificate(s).

7. Delivery period shall be as below:		
(i).	Award of LOI	T0
(ii).	Submission of a detailed design and deployment methodology and implementation plan of execution of the project and the approval of NMDC	T0+1Week
(iii).	Supply of DC / DR Components including hardware and Software.	T0 + 6 Weeks
(iv).	Supply of LAN / WAN Components	T0 + 6 Weeks
(v).	Installation and Commissioning of DC / DR	T0 + 9 Weeks
(vi).	Installation and Commissioning LAN/WAN.	T0 + 15 Weeks

8. Liquidated Damages:	
(i).	PIP shall be required to complete the assigned works within the period stipulated in the RFP. In case of delay which may occur due to the reasons beyond the control of PIP, PIP would approach ITI with full details for extension and time limit for completion of the work.
(ii).	If the delay in completion is attributable to the PIP , PIP shall be liable to pay as Liquidated damages to ITI a sum calculated @ 0.5% of the One Time Cost (supply and installation value) per week of the delay or part thereof subject to a maximum of 10% of the OTC (supply and installation value).
(iii).	Once the delay touches the upper capping of the LD (10%) without any cogent reason, it will be a reason enough to start the process of rescinding the contract and get the work completed by another source/agency at the risk and cost of the PIP.

9. Bank Guarantees:	
(i).	The LOI shall be issued to the selected bidder (PIP) on submission of a Bank Guarantee (BG) for 10% of the total contract value, valid for 18 months, towards successful commissioning of the project.

(ii).	After successful acceptance and commissioning of the project, a Performance Bank Guarantee (PBG) for an amount equal to 5% of the total contract value will be submitted for a period of 63 months towards the warranty and support for smooth operations of the Project and the initial BG {mentioned at (i) above for 10%} shall be discharged.
(iii).	The PBG shall be submitted from a Nationalized Indian Bank/ Scheduled Commercial Bank in the Bank Guarantee formats (model) as enclosed in **Annexure –III** after necessary formative changes, where required**.**

10. Post Implementation:	
(i).	PIP shall hand over all the drawing, technical and operational manuals, software and hardware documentation along with all the software / hardware licenses and other engineering details to the ITI authorized person on completion of the project.
(ii).	The bidder shall ensure that the products (hardware/software etc.) supplied are not at the "End of Life". OEM has to ensure product support at least for a period of 5 years after product is declared End of Life. A declaration in this regard from the OEM to be enclosed in the technical bid.
(iii).	PIP shall provide services as per the SLAs defined for various services in **Annexure - IV** Clause wise compliance to be provided in the technical bid. SLA penalties if any levied on ITI by NMDC, will be recovered from the PIP.
(iv).	PIP should ensure that the deployed technical manpower does not tamper the data or cause any loss/damage to the user department. In case of any such incident or happening the consequences or the loss has to be borne by PIP.

11. Billing and Payment:	
(i).	All bills/invoices shall be raised on ITI Limited – Bangalore.
(ii).	Statutory deductions as applicable will be made while making payment.
(iii).	PIP shall submit all invoices along with supporting documents such as Delivery Challan (Lorry receipt), Installation certificates, Acceptance Certificates, QA certificate and test results of OEM, Completion Certificates, Certified Measurement Books etc.
(iv).	The bidder shall quote their prices on FOR destination basis. Unloading, Unpacking and transportation to the installation sites shall also be borne by the PIP.

12.	**Terms of Payment:**	
(A).	**FOR SUPPLY ITEMS:**	
(i).	**On Placement of Order by ITI**	**20% of Invoice Value.**
(ii).	On Proof of Dispatch	20% of Invoice Value
(iii).	On Receipt of Items at Site	30% of Invoice Value
(iv).	On Installation of The Equipment	20% of Invoice Value
(v).	On Go-Live and Operational Acceptance by NMDC	10% of Invoice Value.
Note: For Item No.**(i)**, payment shall be released, against submission of Bank Guarantee for equivalent amount valid for a period of 6 Months.		
(B).	**For Erection and Commissioning Services (Where Civil works are involved e.g. Cable Laying, Erection of Towers, Earthing Pit, Lightning Arrestors and other Passive Components)**	
(i).	Upon Execution - Monthly Running Bill	90% of Invoice value
(ii).	On Operational Acceptance	10% of Invoice value

(C).	For Recurring Services	
(i).	On certification of work done on quarterly basis	100% of Invoice value

The Payments due, to PIP shall be released on receipt from NMDC as above, on back to back basis through an Escrow account arrangement.

13.	**Important notes**
	13.1 The Company reserves the right to: 13.2 Accept or reject any bid received at its discretion without assigning any reasons whatsoever. 13.2.1 Increase/ decrease/ in quantity or alter the location of installation & commissioning within NMDC premises at any of its Offices / Mining Areas/Sites. 13.2.2 Postpone or extend the above-mentioned dates, without assigning any reason whatsoever. 13.2.3 Demand further qualifications/clarifications/documentations during techno-commercial scrutiny of bids received. 13.3 ITI shall not be responsible for any delay in online submission of bids due to internet/network issues. Hence, bidders are advised to submit their bids well in advance to avoid such situations. 13.4 ITI shall not be liable for any expenses incurred by bidder for delivery of materials or during preparation of bid irrespective of whether it is accepted or not. 13.5 Canvassing i.e. soliciting favour, seeking advantage etc. in any form is strictly prohibited and any bidder if found to have engaged in canvassing, shall be liable to have his bid rejected summarily. 13.6 If the bidder deliberately gives any wrong information in their bid to create circumstances for the acceptance to his bid, ITI reserves the right to reject such bid. **13.7** ITI reserves its rights to modify, add/delete any conditions as deemed required in the RFP on a later stage and such modifications, additions/deletions shall be binding on the bidder/Supplier.
14.	**Force Majeure** PIP shall not be considered in default if a delay in completion of the work occurs due to cause beyond its control such as acts of God, natural calamities, fire, strike, frost, floods, riots and acts of unsurpassed power. PIP shall notify ITI in writing within 10 days from the date of such occurrence. In the event of delay due to such causes, the completion schedule will be extended for a length of time equal to the period of force majeure after getting approval from NMDC. In case of closure of work due to the force majeure, any liabilities towards the PIP and/or expenditure of the PIP shall be payable by ITI after due approval from NMDC.

15.	**Indemnity**
	PIP shall indemnify and hold harmless ITI and its employees from and against any and all suits, actions or administrative proceedings, claims, demands, losses, damages, costs, and expenses of whatsoever nature, including attorney's fees and expenses, in respect of the death or injury of any person or loss of or damage to any property, arising in connection with the offer of services under this LoA and by reason of the negligence of the PIP , or their employees, or agents, except any injury, death or property damage caused by the negligence of NMDC/ITI, its employees, or agents.
16.	**Taxes & Duties**
	16.1 The Bidder / Supplier shall be exclusively responsible for payment of all Taxes, etc., that may be levied from time to time according to the Laws & Regulation now in force & also hereafter to be imposed, increased or modified from time to time. Nothing will be payable extra (except Goods and Service Tax) by the Company in respect of any duties/ taxes to be imposed on procurement of materials for execution of contract.
	16.2 **Goods & Service Tax (GST / IGST)**
	Without prejudice to stipulation in General Conditions of Contract, the quoted price shall be exclusive of Goods and Service Tax. The GST as legally leviable & payable by the Bidder / Supplier under the provisions of applicable law/ act shall be paid extra by the Company as per the Bidder / Supplier's bill. Bid without GST number shall be rejected for Indian Bidders/ authorized Indian agent. At present GST-TDS is applicable. Deduction of GST-TDS at source would be enforced from the running bills at the rates prescribed. The GST (i.e. SGST, CGST or IGST) amount shall be shown separately in invoice and also submit proper Tax Invoice as per section 31 of CGST Act, and Rule 46 of CGST Rules, 2017 to get Input Tax Credit by the Company. Bidder / Supplier shall raise their tax invoice as per contract condition and uploaded their supply invoice in GSTN Portal through GSTR return. Mismatch in return of the Company due to any reason attributable to Bidder / Supplier, the same shall be recovered from Supplier's bill.
	16.3 **New taxes & levies**
	In case Government imposes any new levy / tax after award of the work during the tenure of the contract, the Company shall reimburse the same at actual on submission of documentary proof of payment subject to the satisfaction of the Company that such new levy/tax is applicable to this contract.

| 17. | **Defect Liability (Warranty) Period:** |
| | The defect liability period of the project shall be 12 months from the date of handing over of work (Operational Acceptance). |

(i). PIP shall warrant that the offered BoQ or any part thereof under this LoA shall be free from defects.

(ii). The Defect Liability Period shall be Twelve (12) months from the date of Operational Acceptance. If during the Defect Liability Period any defect be found, PIP shall promptly, in consultation and agreement with ITI and at the cost of PIP, repair, replace or otherwise make good such defect as well as any damage to ITI caused by such defect.

(iii). If the repair, replacement or making good is of such a character that it may affect the efficiency of the Solution or any part thereof, ITI may give to PIP a notice requiring that tests of the defective part of the Solution shall be made by PIP immediately upon completion of such remedial work, whereupon PIP shall carry out such tests. If such an element fails the tests, PIP shall carry out further repair, replacement or making good (as the case may be) until that part of the Solution passes such tests. The tests shall be agreed upon by ITI and PIP. If PIP does not commence the rectification either by repair or replacement of such defects within 30 (thirty) days from the date of notice by ITI or does not complete the rectification with reasonable diligence and within a reasonable time, ITI may, at its option, rectify the defects at PIP 's expense. ITI shall, in such case, deduct from payment due to PIP or from the securities available, the expenses incurred by ITI for remedy of such defects without prejudice to the other rights available to ITI under the LoA.

(iv). If the Solution or any part thereof cannot be used by reason of such defect and/or making good of such defect, the Defect Liability Period of the BoQ/ Solution or such part, as the case may be, shall be extended by a period equal to the period during which the BoQ/ Solution or such part cannot be used by ITI because of any of the aforesaid reasons.

(v). In addition, PIP shall also provide an extended warranty for any such replaced or repaired component for the period of minimum 12 months. Such obligation shall be in addition to the defect liability specified under Clause hereof.

18.	**Arbitration:**
	If the Bidder / Supplier be dissatisfied with the decision of the Company, on any matters in question, dispute or difference on any account or as to the withholding by the Company of any certificates to which the Bidder / Supplier may claim to be entitled to or if the Company fails to make a decisions within a reasonable time (which reasonable time will in no case exceed three months) as the case may be shall demand in writing that such matters in question, dispute or difference be referred to Arbitration. Such demand for Arbitration shall be delivered to the Company by the Bidder / Supplier and shall specify the matters which are in question, dispute or difference and such disputes or difference of which the demand has been made and no other matter shall be referred to arbitration. Provisions of the Arbitration Act 1996 or any statutory modification or re-enactment thereof & the rules made there under & for the time being in force shall apply to the arbitration proceedings. (i) The Arbitration shall have its seat in Bengaluru, Karnataka State, India. (ii). The decision of the Arbitrator shall be final and binding on the parties to this Contract (iii). Each party shall bear its own cost of preparing and presenting its case. The cost of Arbitration including the fees and expenses of the Arbitrator shall be shared equally by the Bidder / Supplier and the Company.
19.	**Jurisdiction of court** The Courts at Bengaluru, Karnataka State, India shall have the exclusive jurisdiction to try all disputes, if any, arising out of this agreement between the parties.
20.	**Sub Contracts** The Bidder / PIP shall not assign or sub-contract the whole or any part of the work awarded to it, without the prior written approval of ITI.
21.	**Insurance** Without limiting any other obligations or liabilities, the PIP shall, at his own costs & risks take and keep comprehensive insurance including third party risk for the plant, machinery, materials etc., brought to the site for all the work during the execution of the contract. The PIP shall also take out workman's compensation insurance as required by law. For any damage/accidents caused during the tenure of the contract, only the PIP is responsible and there will be no liability on ITI.

22.	**Confidentiality:**
	Each Party shall:
	a) use confidential information only for the purposes of this Agreement;
	b) disclose confidential information to a third party only with the prior written consent of the other Party (except that each Party may disclose Confidential Information to its professional advisors or auditors to the extent necessary)
	c) Ensure that any third party (other than the professional advisers or auditors of either Party) to whom confidential information is disclosed executes a confidentiality undertaking.
	22.1. The provisions shall not apply to any confidential information which:
	a) is in or comes into the public domain other than by breach as per mentioned above; or
	b) is or has been independently generated by the recipient party or was in the possession of the recipient party prior to the date of the disclosure.
	22.2 Each party may disclose confidential information pursuant to a statutory obligation, an order of a court of competent jurisdiction or the requirement of a competent regulatory body provided that it notifies the other Party as soon as the requirement to notify arises and shall use its reasonable endeavors to ensure that any such disclosure is made in a manner which ensures the confidentiality of the confidential information.

23.	**Termination of Services//Rescinding of Contract:**

ITI may terminate the services/LOA with immediate effect without prejudice to any other rights or remedies, if:

23.1. PIP, either directly or through their employees or agents or sub-PIP s commits any breach of their obligations hereunder.

    a) PIP, either directly or through their employees, violates the confidentiality of the information of ITI or NMDC Uses or divulges any documents, data, or other information for its own benefit, without the written permission of the other party.

    b) PIP, uses one or more ICT tools such as hardware/software or networking equipment's etc. without prior approval from the other party or uses an unlicensed version of a software

    c) PIP, utilizes the resources of the self or the other party which damages the reputation of the other party or utilizes/ uses the resources in a manner which may incur physical or financial damages/ losses

    d) Such suspension or termination is necessary, in the sole discretion of ITI, to comply with:

- any applicable law, regulation or court order,
- the Rules,
- Security requirements,
- Legal proceeding or settlement which may affect ITI or any of its affiliates.

    e) For non-compliance of Terms and conditions as specified in the RFP

23.2. Before effecting the termination, all the pending financial issues have to be settled between PIP and ITI Ltd.

23.3. In the event of Termination and where the default is attributable to PIP, PIP will do migration/provide knowledge transition of solution, managed services components to service provider chosen by ITI at PIP 's own cost.

23.4. In addition to the above, if the progress of the project does not meet the agreed timelines, then ITI has the right to withdraw this LoA. In such a case, PIP shall peacefully handover all the executed portions of the BoM and other works on 'as is where basis' including all the material (hardware/software/license), documentation and all the records etc. so that implementation of IT infrastructure do not get adversely impacted. In such a situation, PIP shall not be entitled for any compensation and/or claim whatsoever. For non-performance, ITI reserves the right to en-cash the PBG and award work to alternate vendor for completion of the project at risk and cost of the PIP.

24.	**Price Bid Submission.**
	(a). The bidders are required to quote their best itemized prices against the detailed BOQ (Bill of Quantities/Quotes), **Annexure-VI** for each and every section mentioned therein.
	(b). The subtotal of these items also needs to be written in the Bid price sheet at **Annexure-VII** to work out the total package/bid price.
	(c). In case, the amount mentioned against any of the items in annexure VII is different than the total of the BoQs shown in Annexure -VI, the higher of the two shall be taken for bid assessment and lower for the payments, after prorate correction of BoQ.
	(d). The bid with any of the BoQ items as blank shall be termed either as zero or incomplete and bid may be liable for rejection as per the assessment of TEC.
	(e). **Price bid (Annexure-VI & VII), to be put in a separate sealed cover.**
25.	The ultimate motto of whole exercise is successful turnkey commissioning and operation for the next 5 years of the project. Accordingly, the bidder shall include all those items in BOQ (Annexures VI) which it may consider as essential for commissioning of the project but not mentioned in the BoQ or mentioned, but, in less quantity. Such priced added items shall also form part of the total package and needs to be part of the overall worked out price. If the Bidder finds some of the items in BoQ as excessive and reduces them or doesn't quote for them, such item(s) may be asked by ITI to be supplied free of cost by the PIP irrespective of their need in the project. Also, if any of the item neither mentioned in BoQ nor added by the bidder but essentially required in successful commissioning of the project, same shall be supplied by the PIP free of cost.

26. Evaluation of Bids:
The Techno-Commercial bids will be evaluated by a duly constituted Tender Evaluation Committee (TEC) based on the pre-requisite criterion of this RFP. **The Evaluation shall be based on two parameters:** (A). Technical and commercial pre-qualifications (PQ) and (B). Price Bid Bidders, not possessing the minimum eligibility criterion as mentioned in the RFP, will not be assessed further and shall be termed as non-eligible, non-qualifying bid. The TEC will base its recommendations on the information submitted by the bidders as per the RFP terms & Conditions and shall not cast its own assumptions. The TEC may call the bidders to submit additional information or clarifications on the information submitted in their bids. The time limit, in which the bidders' have to submit the additional information, will be decided by the TEC and its decision will be final in this regard. All such communication shall be in writing. Bidders, however shall not be allowed to supplement or supplant any information or bid material at their own after the bid submission date.

27.	**Award of Contract**
	(a). The work shall be awarded to the eligible and qualified bidder with the lowest quoted price (L-1) as per its price bid.
	(b). In case of tie in the price quotes, the bid with lower Price Quoted for supply of DC/DR, inclusive of Hardware and Software shall be preferred.
	(c). ITI reserves the right to negotiate with the L1 bidder in case the quoted price is assessed to be more than reasonable.

28.Financial Quote, on Supply, Installation, Integration, Testing, Commissioning and Support:

S.No	Item	Item wise Sub Total of BoQ
1	DC/DR Hardware	
2	DC/ DR Software	
3	DC DR XMII SW & HW	
4	Fire wall	
5	Switch, EMS, etc..	
6	Wi-Fi & Point to Point radio links	
7	Campus Backbone Cabling	
8	OFC Links	
9	One-time charges for Co-location and Managed Services.	
10	NOC	
11	Co-Location & Managed Services for 5 years	
	TOTAL	

{The BOQs are at **Annexure VI (11 Sheets)** and sub totals needs to be filled up against each item}.

29. Note:

i. Technical bids will be opened on **11/06/2020 at 03.00 pm**.

ii. Price bid opening date will be intimated to the technically qualified bidders separately.

iii. Bid should be valid for a period of 90 days from the date of opening of RFP response.

iv. Conditional offers are liable for rejection.

v. The vendor to indemnify ITI from any claims / penalties / statutory charges, liquidated damages, with legal expenses etc. as charged by the customer.

vi. The bidder shall bear all costs associated with the preparation and submission of his offer against this RFP, including cost of presentation for the purposes of clarification of the offer, if so desired by ITI. ITI will, in no case be responsible or liable for those costs, regardless of the outcome of the RFP process.

30. **Should there be any clarifications, needed before bidding same may be addressed through Email in the following format on or before 17:00 HRS on 27-05-2020 and all clarification shall be obtained before 17:00 HRS on 29-05-2020. Contact person for obtaining clarification shall be:**

<div align="center">

The Deputy General Manager - Corporate MM Department
ITI Limited,
Regd. & Corporate Office,
ITI Bhavan, Dooravaninagar,
Bengaluru – 560 016
Karnataka, India
Email : lokeshpn_crp@itiltd.co.in

</div>

Sl. No.	Clause Nr	Clause Reference	Query
1.			
2.			

31. **Amendment of RFP:** At any time prior to the last date for receipt of offers, ITI, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, modify the RFP document by an amendment. In order to provide prospective bidder reasonable time in which to take the amendment into account in preparing their offers, ITI may, at their discretion, extend the last date for the receipt of offers and/or make other changes in the requirements set out in the Invitation for RFP.

32. **Disclaimer:**

(i). ITI and/or its officers, employees disclaim all liability from any loss or damage, whether foreseeable or not, suffered by any person acting on or refraining from acting because of any information including statements, information, forecasts, estimates or projections contained in this document or conduct ancillary to it whether or not the loss or damage arises in connection with any omission, negligence, default, lack of care or misrepresentation on the part of ITI and/or any of its officers, employees.

(ii). ITI reserves the right to abrogate the process of this RFP at any stage without citing any reason or explanation and without any cost.

(iii). All activities like Proof of concept shall be on "No Cost No Commitment" (NCNC) basis wherever applicable and will be the responsibility of the bidder.

(iv). Bidders would be responsible to comply each and every function as envisaged in the Scope of work including imparting training to ITI personnel (Minimum 20), for smooth day to day Operations and Maintenance of the project.

33. Bidders will be responsible for any shortcoming in the Bill of Material (BOM) and the same should be subsumed in the overall cost and nothing extra shall be payable in order to execute and operationalize the project. All the consumables for the execution, testing, commissioning and support for the project will be to the PIP's account.

34. Successful bidder would open an office in Hyderabad for successful execution of the project and deploy enough manpower to the satisfaction of NMDC for the smooth implementation and maintenance support to the project.

35. **"Selection of IT-Networking Supply and Implementation Partner For Implementation of IT Infrastructure for ERP Implementation and other Future Digital Initiatives at NMDC Locations**"

Ref: CRP20E001   **Date: 20/05/2020**

and to be submitted to the following address on or before **12:00 HRS(IST)** on 11-06-2020.

35.1. Document Submission

The bidders are advised to submit the self-certified documents as called for in the eligibility criteria & follow the pdf signer process in the online tender submission process. However, EMD of Rs 2.0 Crs (Rupees Two Crore only) in the form of DD/Bankers Cheque / BG has to be submitted in original only and has to reach the below mentioned officer/address /**17:00 HRS(IST) on   10-06- 2020**. If BG is submitted in lieu of EMD, the BG shall be from any Indian Nationalized Bank or a Scheduled Bank.

> Purchase Officer - Corporate MM Department,
> ITI Limited, Regd. & Corporate Office,
> ITI Bhavan, Dooravaninagar,
> Bengaluru – 560 016
> Karnataka, India

35.2   Bid submission

Offers should be submitted in favour of:

> The Deputy General Manager - Corporate MM Department
> ITI Limited,
> Regd. & Corporate Office,
> ITI Bhavan, Dooravaninagar,
> Bengaluru – 560 016
> Karnataka, India.

35.3   Bid acceptance

35.3.1   Offers received from the bidders who are failing to meet the eligibility criteria and in deviation from the RFP published, will not be considered.

35.3.2   Offers are to be submitted well within the due date and submission as indicated in this RFP. Late tenders will not be accepted.

ANNEXURE-I

Scope of Work
(refer 1 – 53 pages)

ANNEXURE-II
Technical Specifications
(refer 1 – 127 pages)

ANNEXURE-III

PROFORMA OF BANK GUARANTEE FOR PERFORMANCE
(On non – judicial stamp paper of value not less than ₹ 100 /-)
The non-judicial stamp paper should be in the name of issuing bank

Ref.   Bank Guarantee No.
                                                                     Date. ....20____ .

The Additional General Manager - SZ ITI
Limited
Regional Office / MSP (Karnataka),
F-100, 2nd Floor, East Wing
Dooravaninagar,
Bengaluru - 560 016.

Dear Sirs,

In consideration of the ITI Limited, (herein after referred to as **'ITI'** which expression shall unless repugnant to the Context or meaning thereof include its successors, administrators   and assigns)   having   awarded   to   M/s. _____ with its Registered/Head   office   at _____(here in after referred to as the **'Project Implementation Partner'** (**PIP**) which expression shall unless repugnant to the context or meaning thereof, include its successors, administrators, executors and assigns), a LoI dated_____and the same having been   unequivocally accepted   by the PIP   resulting   in a "LoI" bearing   No._____   dated   _____   valued   at _____for _____(Scope of LoI) and the PIP having agreed to provide a performance guarantee for the faithful performance of the entire LoI equivalent to **-----%** (-------- percent) of the said value of the LoI to the company.

We_____having
                     (Name and Address)
its Head Office at_____(hereinafter referred to as the `Bank', which expression shall, unless repugnant to the context or meaning thereof, include its successors, administrators, executors and assigns) do hereby guarantee and undertake to pay ITI, on demand any and all monies payable by the PIP to the extent of _____ as aforesaid at any time up to _____(days/month/year) without   any demur, reservation, recourse or protest and/or without any reference to the PIP Any such demand made by the ITI on the Bank shall be conclusive and binding not withstanding any difference between ITI and the PIP or any dispute pending before any court, tribunal or any other authority .The Bank undertakes not to revoke this guarantee during its currency without previous consent of the ITI and further agrees that the guarantee herein contained shall continue to be enforceable till the ITI discharges this guarantee.

The ITI shall have the fullest liberty without affecting in any way the liability of the Bank under this guarantee from time to time to extend the time for performance of the contract by the PIP. The ITI shall have the fullest liberty, without affecting this guarantee, to postpone from time to time the exercise of any powers, vested in them or of any right which they might have against the PIP, and to exercise the same any time in any manner, and either to enforce or to for bear to enforce any covenants, contained or implied, in the contract between the ITI or any other course of or remedy or security available to the ITI. The Bank shall not be released of its obligations under these presents by any exercise by the ITI of its liberty with reference to the matters aforesaid or any of them or by reason of any other acts of omission or commission on the part of the ITI or any other indulgence shown by the ITI or by any other matters or thing whatsoever which under law would, but for this provision, have the effect of relieving the Bank.

The Bank also agrees that the ITI at its option shall be entitled to enforce this Guarantee against the Bank as a principal debtor, in the first instance without proceeding against the PIP and not withstanding any security or other guarantee that the ITI.

have in relation the PIP's liabilities.

Notwithstanding anything contained here in above our liability under this guarantee is restricted to _____ and it shall remain in force up to and including _____ * * and shall be extended from time to time for such period (not exceeding one year), as may be desired by M/s._____ whose behalf this guarantee has been given.

Dated this _____ day of _____ 202____ at

_____.

WITNESS

Signature ---------------

Signature
(Name)
----------------------------------- (Name)-----------------
Official address

---Designation with Bank stamp

Attorney as per power of Attorney No.

Dated --------------------------

Annexure-IV
Service Level Agreement

The purpose of the service level agreement (SLA) is to clearly define the levels of service which will be expected from IP during implementation and the subsequent support for the project period.

1. **Definitions**

The purpose of this SLA, the definitions and terms as specified in the LOI and Bid document along with the following terms shall have the meanings set forth below:

- **Incident** – refers to any event / abnormalities in the functioning of the Data Centre / disaster recovery/ specified services that may lead to disruption in normal operations of the services under this LOI/Agreement.

- **Support** – shall mean the support which shall handle patch updates, upgrades Fault Reporting, Trouble Ticketing and resolution of related enquiries during this LOI/Agreement. Interactive remote diagnostic support shall also be there, allowing technical support engineers to troubleshoot an incident securely through a browser-based remote-control feature

- **Availability/Uptime** – shall mean the time for which the services offered are available for conducting operations from the equipment / solution hosted in DC/DR. Availability percentage is measured as

  Availability %age = {(Agreed Service Time – Down Time)/ (Agreed Service Time)} * (100%)

- **Security** - Security incidents could consist of any kind of Malware attacks/ Denial of services/ Intrusion and any kind of security breach including data theft/ loss/ corruption. Security being one of the most important aspects would be governed by standards of MeitY/ CERT-In. All security incidents leading to disruption in availability of the Service would be penalized.

- **Support Channel** – Incident and Helpdesk

  Support is an interface made available by the IP to handle issues and queries raised by

NMDC/ITI. The parameters to measure the performance of the support service does include responsive and timely resolution and reporting of the issues.

- **Disaster Recovery and Data Backup Management**

  This category is usually related to address the business continuity management and disaster recovery. Disaster recovery/ service reliability is the property of DR to provide the services and data availability in the acceptable form, typically over some period of time in case of any disaster. Scheduled downtime and maintenance are normally iron out while designing the service level agreements. It too covers the IP capability to avoid loss of data in case of the any disaster or failures

  The two primary service level agreements which needs to be addressed here are

  i) RPO – recovery point is the maximum allowable time between recovery points and

  ii) RTO – recovery time is the maximum amount of time a business process may be disrupted after the disaster.

- **Scheduled Downtime/ Scheduled Maintenance Time** – shall mean the time that the System is not in service due to a scheduled work. Scheduled maintenance time is planned downtime with the prior permission.

- **Response Time** – Average Time taken to acknowledge and respond, once a ticket/ incident is logged through one of the agreed channels. This is calculated for all tickets/ incidents reported within the reporting month.

- **Resolution Time** shall mean the time taken (after the incident has been reported to the support team) till resolution.

2. **Measurement and Monitoring**

- The SLA parameters shall be monitored on monthly basis as per the individual SLA parameter requirements. However, if the performance of the system/services is degraded significantly at any given point in time during the LOI/Agreement and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of NMDC/ITI or an agency designated by them, then ITI will have the right to take services form another service provider at the cost of IP and/or termination of the LOI/Agreement.

- The Monitoring Tools shall play a critical role in monitoring the SLA compliance and hence will have to be customized accordingly to the requirements of NMDC/ITI. IP shall make available the Monitoring tools for measuring and monitoring the SLAs. IP may deploy additional tools and develop additional scripts (if required) for capturing the required data for SLA report generation in automated way. The tools should generate the SLA Monitoring report in the end of every month which is to be shared with the NMDC/ITI on a monthly basis. NMDC/ITI or its nominated agency shall have full access to the Monitoring Tools/portal (and any other tools / solutions deployed for SLA measurement and monitoring) to extract data (raw, intermediate as well as reports) as required during the project. NMDC/ITI or its nominated agency will also audit the tool and the scripts on a regular basis.

- In case of default on any of the service level metric, the IP shall submit performance improvement plan along with the root cause analysis for NMDC/ITI's approval.

- IP shall submit all the reports pertaining to SLA within 7 working days after end of each quarter.

- All the reports must be made available to NMDC/ITI, as and when the report is generated or as and when asked by the competent authority.

- Agency shall appoint as many team members as deemed fit by them, to meet the time Schedule and SLA requirements.

- During implementation, IP shall ensure that full time team member from each OEM is available till the operational acceptance of their respective BoQ.

3. **Periodic Reviews**

During the LOI/Agreement period, it is envisaged that there could be changes to the SLA, in terms of measurement methodology / logic / criteria, addition, alteration or deletion of certain parameters, based on mutual consent of both the parties, i.e. NMDC/ITI and IP.

- ITI and IP shall ensure that the range of the Services under the SLA shall not be varied, reduced or increased except by the prior written agreement of NMDC/ITI and IP in accordance with the Change Control Schedule.

- The SLAs may be reviewed on an annual basis or at any appropriate time by NMDC/ITI in consultation with the IP.

4. **Penalties**

Payments to the IP to be linked to the compliance with the SLA metrics laid down in the LOI/Agreement.

- The payment will be linked to the compliance with the SLA metrics.

- In case multiple SLA violations occur due to the same root cause or incident, then the SLA that incurs the maximum penalty may be considered for penalty calculation rather than a sum of penalties for the applicable SLA violations

5. **Severity Level**

Below severity definition provide indicative scenarios for defining incidents severity. However, NMDC/ITI will define / change severity at the time of the incident or any time before the closure of the ticket based on the business and compliance impacts.

Severity Level	Description	Examples
Severity 1: **Critical**	Environment is down or major malfunction resulting in an inoperative condition or disrupts critical business functions and requires immediate attention. A significant number of end users (includes public users) are unable to reasonably perform their normal activities as essential functions and critical programs are either not working or are not available	- Non-availability of VM. - No access to Storage, software or application
Severity 2 **High**	Loss of performance resulting in users (includes public users) being unable to perform their normal activities as essential functions and critical programs are partially available or severely restricted. Inconvenient workaround or no workaround exists. The environment is usable but severely limited.	- Failure of Network Connectivity, virus on many devices, Local File/Server and Backup
Severity 3 **Medium**	Moderate loss of performance resulting in multiple users (includes public users) impacted in their normal functions.	- Failure of a department/group or a floor, an application meant for a particular department or user group.
Severity 4 **Low**	A problem that affects entire Organization/Network/Critical Application/ Group/People	- Minor Bug fixes, new software installation and upgrades

6. Service Level Agreements (SLA)

#	Parameter	Target	Basis	Penalty
Availability/ Uptime				
1.	Availability/ Uptime of each server at DC/DR	Availability for each server>=99.95% per quarter	Calculate based on no. of SLAs breach with in one quarter	Penalty as indicated below (per occurrence) a) <99.95% to >=99.5% **0.125% of Quarterly ARC for Colocation and Managed Services** b) < 99.5% to 98% **0.25% of Quarterly ARC for Colocation and Managed Services** c) < 98% **0.5% of Quarterly ARC for Colocation and Managed Services** In case of 2 consecutive Quarterly SLA breach under Point c), ITI has the right to invoke the termination clause.
2.	Availability of the network links at NMDC locations including DC/ DR	Availability for each of the network links: >= 99.5%	Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the DC Calculated based on no of SLA breaches per month per NMDC project locations	Default on any one or more of the provisioned network links will attract penalty as indicated below. a) <99.5% &>=99% **1% of Quarterly ARC for Bandwidth** b) < 99% to 98% **2% of Quarterly ARC for Bandwidth** c) < 98% **5% of Quarterly ARC**

				for Bandwidth
				In case of 2 consecutive Quarterly SLA breach under Point c),ITI has the right to invoke the termination clause.

Support Channels - Incident and Helpdesk

3	Response Time	95% within 15 minutes during Business Hours And 95% within 60 minutes during Non-Business Hours	This is calculated for all tickets/ incidents reported within the reporting month.	a) <95% &>=90% **1% of Quarterly ARC for Man Power** b) <90% &>=85% **2% of Quarterly ARC for Man Power** c) < 85% &>= 80% **5% of Quarterly ARC for Man Power**
4	Time to Resolve - **Severity 1**	For Severity1, 98% of the incidents should be resolved within 120 Minutes of problem reporting	Time taken to resolve the reported ticket/incident from the time of logging. This is calculated for all tickets/ incidents reported within the reporting month.	<98% &>=90% **2% of Quarterly ARC for Man Power** < 90% &>= 85% **5% of Quarterly ARC for Man Power** < 85% &>= 80% **8% of Quarterly ARC for Man Power**
5	Time to Resolve - **Severity 2,3**	95% of Severity 2 within 8 hours of problem reporting AND 95% of Severity 3 Within 24 hours of problem reporting	Time taken to resolve the reported Ticket/incident from the time of logging. This is calculated for all tickets/incidents reported within the Reporting month.	95% &>=90% **0.5% of Quarterly ARC for Man Power** < 90% &>= 85% **1% of Quarterly ARC for Man Power** < 85% &>= 80% **2% of Quarterly ARC for Man Power**

6	Time to Resolve - **Severity 4**	95% of Severity 4 within 48 hours of problem reporting	Time taken to resolve the reported Ticket/incident from the time of logging. This is calculated for all tickets/incidents reported within the Reporting month.	95% &>=90% **0.25% of Quarterly ARC for Man Power** < 90% &>= 85% **0.5% of Quarterly ARC for Man Power** < 85% &>= 80% **1% of Quarterly ARC for Man Power**
Security Incident and Management Reporting				
7	Percentage of timely incident report	Within 1 hour	Measured as a percentage by the number of defined incidents reported within a predefined time (1 hour) limit after discovery, over the total number of defined incidents which are reported within a predefined period (i.e. month). Incident Response - MSP shall assess and acknowledge the defined incidents within 1 hour after discovery	<95% &>=90% **1% of Quarterly ARC for Colocation and Managed Services** <90% &>=85% **2% of Quarterly ARC for Colocation and Managed Services** < 85% &>= 80% **3% of Quarterly ARC for Colocation and Managed Services**
8	Percentage of timely incident resolutions	95% to be resolved within 1 hour	Measured as a percentage of defined incidents that are resolved within a predefined time limit (month) over the total number of defined incidents within a predefined period. (Month). Measured from	<95% &>=90% **1% of Quarterly ARC for Colocation and Managed Services** <90% &>=85% **2% of Quarterly ARC for Colocation and Managed Services**

			Incident Reports	
				< 85% &>= 80% **5% of Quarterly ARC for Colocation and Managed Services**
Security				
9	Security breach including Data Theft/Loss/Corruption	No Breach	Any incident where in system compromised or any case wherein data theft occurs (including internal incidents)	For each breach/data theft, penalty will be levied as per following criteria. Any security incident detected INR 5 Lakhs. This penalty is applicable per incident. These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security wherein the data is stolen or corrupted, ITI reserves the right to terminate the LOI/Agreement.
Service levels for Disaster Recovery				
10	Recovery Point Objective (RPO)	<= 30 Minutes	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	For every 30 Minutes or part there of delay: **2% of Quarterly ARC for Colocation and Managed Services**
11	Recovery Time Objective (RTO)	<=4 Hours	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	For every 2 Hours or part thereof delay: **2% of Quarterly ARC for Colocation and Managed Services**

Annexure-V

BID SECURITY/ EMD Guarantee
(To be typed on Rs.100/- non-judicial stamp paper)

To

ITI Limited, Dooravaninagar,
Bangalore-560016.

Sub: Bid Security/EMD guarantee.

Whereas ....(herein after referred to as Bidder) has approached us for Giving Bank Guarantee of **Rs./-(Rupees Only)** (here after known as the" B.G. Amount") **valid up to ……….** (hereafter known as the "Validity date") in favour of ITI Limited, Bangalore Herein after referred to as ITI) for participation in the tender of work of…………….…Now at the request of the Bidder, We...Bank …………………………Branch having ………………………………………… ………. …………………………………. (Address) and Regd. office address as ……… ………...…………………………………………………………………… ……… ……… …………… (Hereinafter called 'the Bank') agrees to give this guarantee as hereinafter contained:

1. We the Bank do hereby undertake to pay the amounts due and payable under this guarantee without any demur, merely on a demand from the ITI stating that the amount claimed is due by way of loss or damage caused to or would because door suffered by the ITI by reason of breach by the said BIDDER of any of terms or conditions contained in the said Agreement or by reason of the BIDDER failure to perform the said Agreement. Any such demand made on the bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee where the decision of the ITI in these counts shall be final and binding on the bank. However, our liability under this guarantee shall be restricted to an amount not exceeding the "B.G. Amount".

2. We undertake to pay to the ITI any money so demanded not withstanding any dispute or disputes raised by the BIDDER in any suit or proceeding before any court or tribunal relating thereto our liability under this present being absolute and unequivocal. The Payment so made by us under this bond shall be valid discharge of our liability for payment there under and the BIDDER shall have no claim against us for making such payment.

3. We the Bank further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said agreement and that it shall continue to been forceable till all the dues of the ITI under or by virtue of the said Agreement have been fully paid and its claims satisfied or discharged or till ITI certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said BIDDER and accordingly discharge this guarantee. Unless a demand or claim under this guarantee is made on us in writing or before the expiry of Validity date from the date hereof, we shall be discharged from all liability under

this guarantee thereafter.

4. We the Bank further agree with the ITI that the ITI shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said Agreement or to extend time of performance by the said BIDDER from time to time or to postpone for any time or from time to time any of the powers exercisable by the ITI against the said BIDDER and to for bear or enforce any of the terms and conditions relating to the said agreement and we shall not be relieved from our liability by reason of any such variation, or extension being granted to the said BIDDER or for any forbearance, act or omission on the part of the ITI or any indulgence by the ITI to the said BIDDER or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.

5. Notwithstanding anything here in contained;
(a) The liability of the Bank under this guarantee is restricted to the "B. G. Amount" and it will remain in force up to its Validity date specified above.
(b) The guarantee shall stand completely discharged and all rights of the ITI under this Guarantee shall be extinguished if no claim or demand is made on us in writing on or before its validity date.

6. In case ITI demands for any money under this bank guarantee, the same shall be paid through banker's Cheque in favour of "ITI Limited, Bangalore" payable at Bangalore.

7. The Bank guarantees that the below mentioned officer who have signed it on behalf of the Bank have authority to give this guarantee under its delegated power.

Notwithstanding anything contained herein:

1. Our liability under this Bank Guarantee shall not **Rs.   /- (Rupees   Only)**

2. This Bank Guarantee shall be **valid up to…..**

3. We are liable to pay the guarantee amount or any part thereof under this Bank Guarantee only if you serve upon us a written claim or demand on or before**……………**

(date of expiry of guarantee)

Place: ……………………………

Date:……………………………..   (Signature of the Bank Officer)

Rubber stamp of the bank

Authorized Power of Attorney Number: Name of the Bank officer:

Designation:

Complete Postal address of Bank: Telephone Numbers.

Fax numbers

Annexure-VI

(Refer 11 excel sheets)
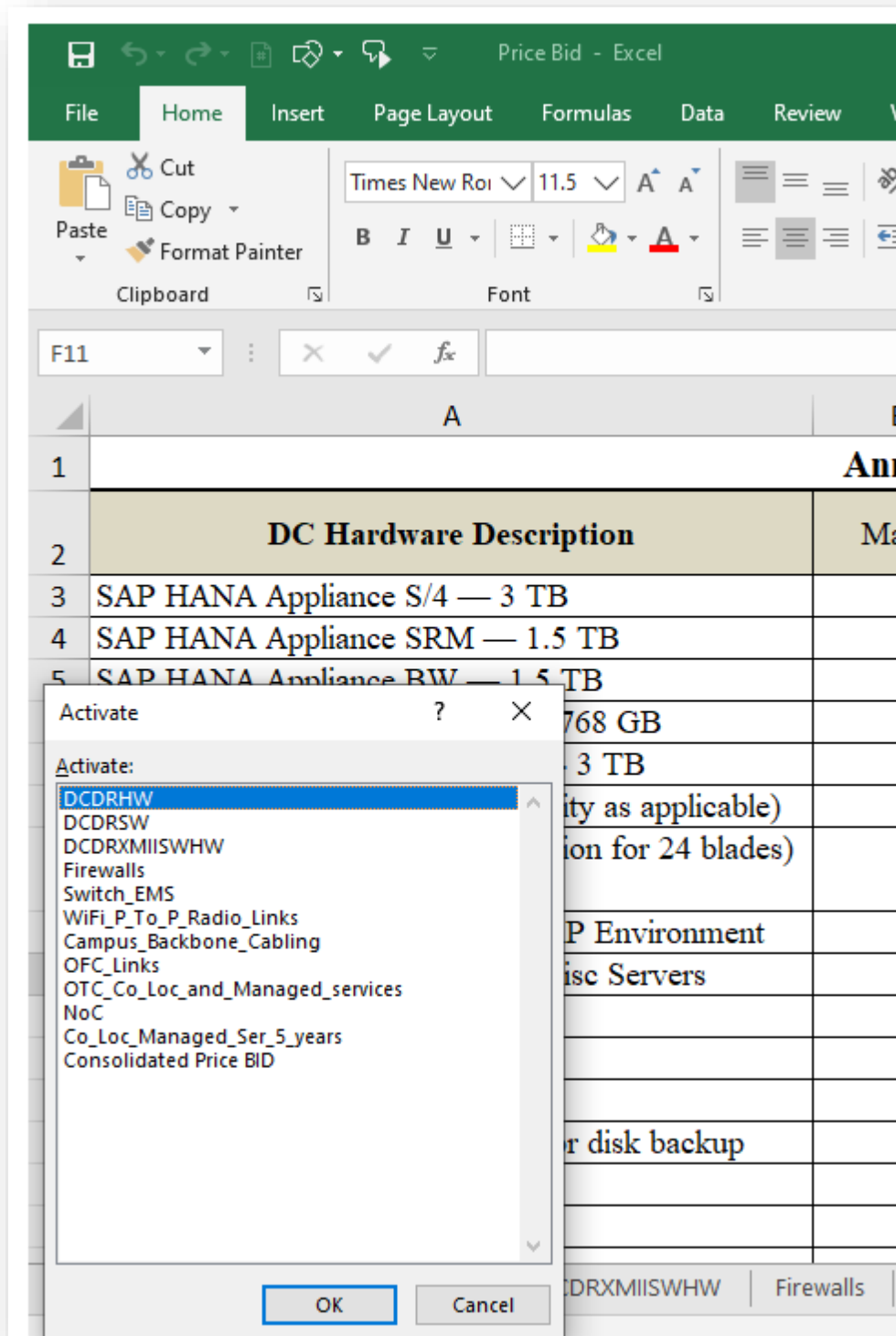
Annexure-VII

(Consolidated Price Bid)

S.No	Item	Item wise Sub Total of BoQ
1	DC/DR Hardware	
2	DC/ DR Software	
3	DC DR XMII SW & HW	
4	Fire wall	
5	Switch, EMS, etc..	
6	Wi-Fi & Point to Point radio links	
7	Campus Backbone Cabling	
8	OFC Links	
9	One-time charges for Co-location and Managed Services.	
10	NOC	
11	Co-Location & Managed Services for 5 years	
	TOTAL	

Note: **(You can refer the above Consolidated Price Bid as Excel Sheet at end of the BoQ sheet/s) * The same data should submit as Annexure-VII)**

Annexure-VIII

Non-Disclosure Agreement
(Between M/s ………. & ITI Ltd)

This Agreement is made between:

xxxxx, a Company incorporated under the Companies Act, 1956, having its Registered Office at ………………………………………, CIN No - …………………………….. (hereinafter referred to as "XXX" which shall include its successors and permitted assigns, herein after referred to as IP);

and

ITI Limited, a Company incorporated under the Companies Act, 1956 having its Registered & Corporate Office at ITI Bhavan, Dooravaninagar Bangalore - 560016, INDIA, CIN No: L32202KA1950GOI000640 (hereinafter referred to as "ITI" which shall include its successors and permitted assigns).

xxxxxxxxxxxxx and ITI are hereinafter also referred to individually as "Party" and collectively as "Parties".

Background:

The Parties are evaluating and negotiating a potential contractual relationship, subject to mutually agreed definitive agreement, as per RFP No. ---------------due on ……. issued by ITI Limited for "………………………………………………………………………………………" (the "Project").

(A)   XXX may in these evaluations and negotiations disclose certain Confidential Information (as defined below) to Company;

(B)   The Parties agree that the disclosure and use of Confidential Information is to be made on the terms of this Agreement.

The Parties agree as follows:

1   Definitions

In this Agreement, the following definitions apply:

"Affiliate" means, at the time of disclosure of any Confidential Information, any legal entity that directly or indirectly controls, is controlled by, or under common control with, a Party.

"Agreement" means this Non-Disclosure Agreement, as amended from time to time under Section 8.

"Confidential Information" means any information that is disclosed or made available in any form by XXX to Company, or that Company has gained knowledge from XXX as a result of this Agreement, but only if:

(a)   such information is disclosed by XXX in writing, it is marked as confidential on disclosure;

(b)   such information is disclosed by XXX orally, it is identified as confidential on disclosure;

(c)   such information is disclosed in any other manner, it is designated in writing as confidential on disclosure; or

(d)   the nature of such information otherwise makes it clear that it is confidential;

but excludes information that:

(e)   is or becomes publicly available, except by an act or omission of Company,

(f)   is demonstrably developed at any time by Company without use of such information, or

(g)   is lawfully obtained at any time by Company from a third party without restrictions in its disclosure or use.

"Project" means the project defined under (A) in "Background".

"Purpose" means the evaluations and negotiations of a contractual relationship between the Parties for the Project.

2   Non-disclosure of Confidential Information

2.1   Subject to Section 4, Company must not disclose Confidential Information to any third party.

2.2   Company is liable for:

2.2.1   its loss or its unauthorized disclosure of Confidential Information, and

2.2.2   any loss or unauthorized disclosure of Confidential Information by any person that Company may disclose and has disclosed Confidential Information to under this Agreement.

2.3   But Company is not liable under Section 2.2 if both of the following conditions are fulfilled:

2.3.1   Company has used the same degree of care in safeguarding the Confidential Information as it uses for its own similar confidential information, but not less than a reasonable degree of care; and

2.3.2   Company notifies XXX immediately after it becomes aware of such inadvertent or unauthorized disclosure and takes reasonable measures to mitigate the effects of such disclosure and to prevent any further disclosure.

3   Use of Confidential Information

3.1   Company shall only use the Confidential Information for the Purpose.

3.2   The Confidential Information is provided "as is" without warranty of any kind and will remain the property of XXX.

3.3   Nothing in this Agreement assigns or transfers XXX's intellectual property rights in any Confidential Information to Company.

4   Permitted Disclosure of Confidential Information

4.1   Company may only disclose Confidential Information to its employee, consultant or Affiliate if the disclosure is necessary for the Purpose.

4.2   Company may disclose Confidential Information to its Affiliate or consultant, and the Affiliate or the consultant is entitled to use the Confidential Information, but only if:

4.2.1   the Affiliate or consultant uses the Confidential Information to the same extent as Company may under this Agreement; and

4.2.2   Company undertakes that any Affiliate or consultant that receives Confidential Information will comply with this Agreement or with separate confidentiality obligations as restrictive as this Agreement.

4.3   Subject to 4.2, Company may disclose Confidential Information to any other third party, but only if:

4.3.1   XXX consents in writing before disclosure; and

4.3.2   Company undertakes that any such third party that receives Confidential Information will comply with this Agreement or confidentiality obligations as restrictive as this Agreement.

4.4   Company may disclose Confidential Information if:

4.4.1   such disclosure is in response to a valid order of a court or any other governmental body having jurisdiction over this Agreement, or

4.4.2   such disclosure is otherwise required by law or the rules of any stock exchange on which the shares or other securities of either party or its Affiliates are listed,

but only if (to the extent possible) Company has first given prior written notice to XXX and made reasonable efforts to protect the Confidential Information on such disclosure.

5   Copying and return of furnished instruments

5.1   Company may not copy any instruments furnished by XXX and containing Confidential Information, unless and to the extent necessary for the Purpose.

5.2   Any models, computer programs, documents and other instruments containing Confidential Information remain XXX's property. Company shall at its own cost return or destroy any such instruments or its copies at XXX's request.

6   Non-disclosure of negotiations

Subject to Section 4, neither Party may disclose to any third party the fact that the parties are evaluating and discussing the Project, without the other Party's consent. This undertaking survives the termination of this Agreement.

7   Term and termination

7.1   This Agreement comes into force on the day that both Parties duly sign it. But this Agreement applies to any Confidential Information that may have been disclosed before this time in connection with the Purpose.

7.2   This Agreement terminates Five (5) years after the date both Parties signed it or earlier, if it is superseded by stipulations of any future agreement between the Parties for the Project or if the Parties decide to end the Project. Notwithstanding the above, the rights and obligations set forth in this Agreement which have accrued prior to termination shall survive the termination or earlier expiration of this Agreement for a period of five (5) years.

8   Amendments

This Agreement may only be amended or modified by written agreement between the Parties.

9   Governing law and arbitration

10   ARBITRATION

10.1   The Parties shall make best efforts to settle any/all disputes amicably within 30 days of communications thereof.

10.2   All disputes or differences whatsoever, arising out of this NDA including the interpretation of any provisions shall be settled by arbitration in accordance with the provisions of Indian Arbitration and Conciliation Act, 1996. The Arbitration panel contains three Arbitrators, one to be appointed by the ITI and the other by XXX and the third Arbitrator shall be appointed by Arbitrators appointed as above. The decision of the Arbitrators will be binding on all the Parties to this NDA. The language of the Arbitration Proceedings shall be English. The place of Arbitration Proceedings shall be Bangalore, India.

10.3   The above clauses on Arbitration shall survive for three (03) years even after the expiry/termination of NDA.

10.4   It is expressly understood and agreed by and between XXX and ITI that ITI is entering into this NDA solely on its own behalf and not on behalf of any other person or entity. In particular, it is expressly understood and agreed between the Parties that the Government of India is not a party to this NDA and has no liabilities, obligations or rights hereunder. It is hereby expressly understood and agreed that ITI is an independent legal entity with power and authority to enter into contracts solely on its own behalf under the applicable Laws of India and general principles of Contract Law. ITI represents and XXX expressly agree, acknowledge and understand that ITI is not an agent,

representative or delegate of the Government of India. It is further understood and agreed between the Parties that the Government of India is not and shall not be liable for any acts, omissions, commissions, breaches or other wrongs arising out of the contract. Accordingly, XXX hereby expressly waive, release and forego any and all actions or claims, including cross claims, impleader claims or counter claims against the Government of India arising out of this contract and covenants not to sue the Government of India as to any manner, claim, cause of action or thing whatsoever arising of or under this NDA.

The Parties have signed two identical copies of this Agreement and have taken one copy each.

For and on behalf of   For and on behalf of
ITI Limited   XXXXXX
(Authorized Signatory)   (Authorized Signatory)
Name: Name:
Designation: Designation:

Annexure-IX

PRE-CONTRACT INTEGRITY PACT

GENERAL

This pre-bid pre-contract agreement (hereinafter called the Integrity Pact) is made on day of ……….... the month of ……..., between, ITI Limited, ITI Bhavan, Dooravaninagar, Bangalore – 560016, India, (hereinafter called the "ITI", which expression shall mean and include, unless the context otherwise requires, his successors in office and assigns) of the First Part and M/s …………….…… (*address of the intending bidder*) (hereinafter called the "Bidder " which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

WHEREAS the BUYER proposes to invite Request For Proposal (RFP) for selection/ empanelment of technology partner for a technical tie-up with ITI for the marketing/manufacturing of ……………… ….. (*name of the product*) and the IP is willing to participate in the RFP as per the terms and conditions mentioned thereon;

WHEREAS the IP is a private company/public company/Government undertaking/partnership company (*strike off whichever is not applicable*), constituted in accordance with the relevant law in the matter and the BUYER is a PSU under the Department of Telecommunications, Ministry of Communications & IT, Government of India.

NOW, THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence/prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to: -

Enabling the BUYER to select/ empanel a technology partner for the marketing/ manufacturing of …. (name of the product) through the RFP in a transparent and corruption free manner, and

Enabling IPs to abstain from bribing or Indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the BUYER will commit to prevent corruption, in any form, by its officials by following transparent procedures.

The parties hereto hereby agree to enter into this Integrity Pact and agree as follows:

1. Commitments of the BUYER
1.1 The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the IP, either for themselves or for any person, 'organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

1.2 The BUYER will during the pre-contract stage, treat all IPs alike, and will provide to all IPs the same information and will not provide any such information to any particular IP which could afford an advantage to that particular IP in comparison to other IPs.

1.3 All the officials of the BUYER will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

2 In case any such preceding misconduct on the part of such official(s) is reported by the IP to the BUYER with full and verifiable facts and the same is prima facie found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the BUYER and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings under the contract would not be stalled.

3 Commitments of IP
3.1 The IP commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following: -

a) The IP will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

b) The IP further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or, execution of the contract or any other contract with the Government for showing or forbearing to show favour or disfavor to any person in relation to the contract or any other contract with the Government.

c) IPs shall disclose the name and address of agents and representatives and Indian IPs shall disclose their foreign principals or associates.

d) IPs shall disclose the payments to be made by them to agents/ brokers or any other intermediary, in connection with this bid/contract.

e) The IP further confirms and declares to the BUYER that the IP is the original manufacturer/ integrator and has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the IP, nor has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such, intercession, facilitation or recommendation.

f)   The IP either while presenting the bid or during pre-contract negotiations or before signing the contract, shall 'disclose any payments he has made, is committed to or intends to make to officials of the BUYER or their· family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

g)   The IP will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

h)   The IP will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

i)   The IP shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the BUYER as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The IP also undertakes to exercise due and adequate care lest any such information is divulged.

j)   The IP commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

k)   The IP shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

l)   If the IP or any employee of the IP or any person acting on behalf of the IP, either directly or indirectly, is a relative of any of the officers of the BUYER, or alternatively, if any relative of an officer of the BUYER has financial interest/stake in the IP's firm, the same shall be disclosed by the IP at the time of filing of tender. The term 'relative' for this purpose would be as defined in Section 6 of the Companies Act 1956.

m)   The IP shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the BUYER.

4   Previous Transgression
4.1   The IP declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect of any 'corrupt practices envisaged hereunder or with any Public-Sector Enterprise in India or any Government Department in India that could justify IP's exclusion from the tender process.

4.2   The IP agrees that if it makes incorrect statement on this subject, IP can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

5   Sanctions for Violations
5.1   Any breach of the aforesaid provisions by the IP or anyone employed by it or acting on its behalf (whether with or without the knowledge of the IP) shall entitle the BUYER to take all or any one of the following actions, wherever required: -

a) To immediately call off the pre-contract negotiations without assigning any reason or giving any compensation to the IP. However, the proceedings with the other IP(s) would continue.

b) To immediately cancel the contract, if already signed, without giving any compensation to the IP.

c) To cancel all or any other Contracts with the IP. The IP shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission.

d) To recover all sums paid in violation of this Pact by the IP(s) to any middleman or agent or broker with a view to securing the contract.

5.2 The BUYER will be entitled to take all or any of the actions mentioned above, also on the Commission by the IP or anyone employed by it or acting on its behalf (whether with or without the knowledge of the IP), of an offence as defined in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

5.3 The decision of the BUYER to the effect that a breach of the provisions of this Pact has been committed by the IP shall be final and conclusive on the IP. However, the IP can approach the Independent Monitor(s) appointed for the purposes of this Pact.

6   Independent Monitors
6.1   The BUYER appoints Independent Monitor (hereinafter referred to as Monitor) for this Pact in consultation with the Central Vigilance Commission.

6.2   The task of the Monitor shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.

6.3   The Monitor shall not be subject to instructions by the representatives of the parties and perform their functions neutrally and independently.

6.4   Both the parties accept that the Monitor have the right to access all the documents relating to the project/procurement, including minutes of meetings.

6.5   As soon as the Monitor notices, or has reason to believe, a violation of this Pact, he will so inform the Authority designated by the BUYER.

6.6   The IP(s) accept(s) that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the IP. The IP will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The Monitor shall be under contractual obligation to treat the information and documents of the IP with confidentiality.

6.7   The BUYER will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual

relations between the parties. The parties will offer to the Monitor the option to participate in such meetings.

6.8 The Monitor will submit a written report to the designated Authority of BUYER within 8 to 10 weeks from the date of reference or intimation to him by the BUYER *I* IP and, should the occasion arise, submit proposals for correcting problematic situations.

7 Facilitation of Investigation
7.1 In case of any allegation of violation of any provisions of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the IP and the IP shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

8 Law and Place of Jurisdiction
8.1 This Pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the BUYER.

9 Other Legal Actions
9.1 The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

10 Validity
10.1 The validity of this Integrity Pact shall be from date of its signing and extend up to the contract period with the BUYER in case a contract is signed. In case IP is unsuccessful, this Integrity Pact shall expire after six months from the date of the signing of the contract.

10.2 Should one or several provisions of this Pact turn out to be invalid, the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intentions.

11 The parties hereby sign this Integrity Pact.

BUYER   IP
Name of the Officer.   CHIEF EXECUTIVE OFFICER
Designation   M/s …. (address)
ITI Limited (address)
Place: Place:
Date: Date:

Witness:

1. ………..   1. …………
2. ………..   2. ………….

Annexure-X

Declaration that the Bidder has not been blacklisted/debarred

(To be submitted on Non-Judicial Stamp Paper of Rs. 100/- duly notarized)

Place:
Date:
To,
<name and address>
Ref: RFP Notification no   dated
Subject: Declaration of Bidder being not blacklisted

Dear Sir,

It is certified that our firm/company or any of our entity is **not** black listed/Debarred from doing business or put on holiday list etc by any Govt. Organization / PSUs for any reason. However, if we fail to complete the awarded work / fulfill the RFP conditions or if any of the information submitted by our company or its employee or associate, proves to be false, ITI Ltd shall be free to take action / black list our firm / company notwithstanding of taking any other legal action."

Place   :
Date   :
Bidder's Company Seal   :
Authorized Signatory's Signature   :
Authorized Signatory's Name and Designation:

ANNEXURE: XI

Manufacturer Authorization Form (MAF)

The Sole Bidder or lead bidder should submit valid Letter with (MAF) with undertaking from the OEM of the vendors whose product is being quoted by the bidder, as detailed in the RFP. The MAF from the OEM issued to the sole bidder or lead bidder shall contain the complete details of OEM such as Name of OEM, Address of Registered office and works, Details of product Details etc. MAF must also contain declaration confirming the following:

OEM shall ensure that all equipment/components/sub- components being supplied by them shall be supported for the entire contract period.

The MAF shall be submitted separately for each item irrespective of same or different OEM. Bidder can submit different authorization for different item and can select different OEM for different item. The following details are to be submitted in (MAF) **Manufacturer Authorization Form**:

1. Name of company :

2. Product Details :

3. Status of Approvals of Standardization Institutions :

4. Years of Experience in supply and Maintenance, of equipment quoted

5. Production Capacity :

I hereby undertake that if M/s _____ ____, address _____ is successful in the ITI Ltd RFP No. …………………………………….. Dated ….04.2020, invited by M/s ITI Ltd for NMDC Project, we will supply the items mentioned in the bid (BoQ) including spares, within the contract period. We further undertake to continue service & support during entire execution, warranty and Operation & Maintenance period. We hereby extend our full guarantee and warranty for the goods offered for supply by the above company against this project.

<div align="right">

Seal & Signature of OEM
Address
Dated:

</div>

Annexure-XII

Details of MAF Required

Sl. No.	Type	Description	MAF Required
Data Center & Disaster Recovery Site			
a)	Hardware		
		HANA Boxes	Yes
		Servers	Yes
		Blade Enclosures	Yes
		Storage	Yes
		Switches	Yes
		Tape Library	Yes
b)	Software		
		Microsoft Windows	Yes
		SLES	Yes
		SLES for SAP Applications	Yes
		Vmware	Yes
		EMS	Yes
		Backup	Yes
Networking			
a)	Active		
		Firewalls	Yes
		Switches (Core, Distribution, Access)	Yes
		NAC	Yes
		Outdoor Wifi	Yes
		Indoor Wifi	Yes
b)	Passive		
		Optical Fiber Cable	Yes
		LIU's	Yes
		UTP Cables	Yes
		Jack Panels	Yes
		I/O's	Yes
		Patch Cords	Yes
		Racks	Yes
Others			
a)	Electrical		
		UPS's	Yes

ITI LIMITED

(A Government of India Undertaking)

COMPLIANCE STATEMENT

NIT Reference No: CRP20E001   Dated: 20.05.2020

**Selection of an Experienced IT-Networking Partner
For
IT Infrastructure Implementation for ERP and other Future Digital Initiatives at NMDC Locations.**

Supplier Name & Address:	
Phone No. & Email Id	

Clause No.	Description	Compliance (Yes/No)
1)	**Scope of the Work**	
a	Establishment of a DC (Data Centre) and DR (Disaster Recovery Centre) (on Co-Location basis at MeitY Empaneled Service Provider) to host the Applications of NMDC such as SAP S/4 HANA ERP at DC, located in Hyderabad and DR located in another city and another seismic zone.	
b	Supply, Installation, Integration, Testing, Commissioning and Support (SiitcS) of LAN and WAN Networks.	
c	Provide/ Upgrade existing MPLS/ VPN at 15 locations of NMDC namely: i. NMDC HO, Hyderabad ii. Kirandul Iron Ore Mining Complex, Dantewada, Chhattisgarh iii. Bacheli Iron Ore Mining Complex, Dantewada, Chhattisgarh iv. Donimalai Iron Ore Mining Complex, Bellary, Karnataka v. NISP, Jagdalpur, Chhattisgarh vi. DMP, Panna, Madhya Pradesh vii. R&D Centre, Hyderabad viii. SIU, Paloncha ix. GEC, Raipur x. RO, Visakhapatnam xi. RO, Bhubaneswar xii. RO, New Delhi. xiii. RO, Chennai xiv. RO, Bengaluru xv. RO, Kolkata	
d	To submit a detailed design and deployment methodology and plan of execution of the project for the approval before its implementation.	
e	Integrate / upgrade Internet Leased Lines (ILL) at HO, Projects and other locations of NMDC.	
f	Deployment of secured security solutions	
g	Provision of secured encrypted VPN over the internet for remote access to applications	
h	Inter Connecting the nodes with Optical fiber or Radio links, including supply, installation, integration, testing, commissioning and maintenance support (SiitcS)	
	(Detailed Scope of work to be referred for compliance, is enclosed at Annexure-I).	
	Note: 5 Years Comprehensive Warranty and maintenance support needs to be provided to all the elements of network.	
	The required MPLS and ILL connectivity from the TSPs shall be arranged separately and bidder need not to account for its cost.	
	(Technical Specifications are enclosed at **Annexure-II**)	
2)	**Eligibility Criteria**	
a.	The bidder must be, a company registered in India, under the companies Act – 1956 or 2013 and should be in business of IT / ITI ES/Networking for at least 5 years.	
b.	Average Annual financial turnover during the last 3 years, ending 31st March-2019 should be at least Rs. 100 Cr . Audited financial statements for the last 3 years (2016-17, 2017-18, 2018-19) to be enclosed.	
c.	The bidder should be financially strong having Positive Net worth in each of the last 3 financial years.	
d.	The intending bidder must be an IT/ITES/Networking company, having an Experience of successfully executing similar nature of works as mentioned in the Scope of Work viz. setting up of DC/DR (H/w & S/w), Firewalls, active Switches, Managed Services, Backbone cabling, Setting up of Wi-Fi Networks, laying of WAN/LAN Networks and laying of OFC etc. during the last 7 years (as on 31st March'2020) of at least following value/billing: **One Project costing Rs 80 Cr OR Two projects costing Rs 50 Cr. each OR Three Projects costing Rs 40 Cr. each.** The project/projects claimed towards experience, must contain one or more elements essentially from each of the following three categories. Elements of Category (i) below, must contribute at least 30% cost of the project.	
	i) The establishment of DC/DR, Fire-walls and Managed services.	
	ii) Active Switches, EMS and Backbone Cabling with associated IT components.	
	iii) Wi-Fi, P2P radio links and Laying of Underground OFC Networks.	
	(Project-Wise, Work order copies and completion certificates, depicting various project elements and costs thereof, with MAF details, to be enclosed).	
e.	IT Service & Security Accreditations: The intending bidder must possess the following certifications on the date of submission of the bids:	
	i) Valid ISO 20000 Certificate	
	ii) Valid ISO 27000 Certificate	
	iii) Valid CMMi Level 3 or above, certificate	
f.	The bidder should have MAF from respective OEM(s) for addressing this RFP, which it proposes to use in this project.	
g.	Authorization letters from OEM's concerned (MAF) to address this business opportunity needs to be enclosed in the given format. Bids without authorization will not be considered. List of MAF.s required is at **Annexure-XII**	
h.	The bidder should not have been black listed by central / state governments / PSUs as on date of bid submission. Self-certificate shall be submitted in this regard. **(Annexure-X)**	
i.	Bidders must quote for one of the brands of the equipment as identified by the user and mentioned in the technical specs / Bill of Material. No other brand will be considered.	
j.	The bidder shall submit an undertaking that they do not have any ongoing disputes on statutory levies like Income Tax, GST, PF, ESI etc.	
k.	Authorization letter in company letter head authorizing the person signing the Bid for this RFP.	
l.	Clause by Clause compliance of RFP terms & conditions needs to be submitted. Non-compliance on technical specifications and offers with deviations are liable to be rejected.	

Annexure – I : Scope of Work

1 Background and Scope

1.1   Scope of Work

The minimum specified scope of work to be undertaken shall be for Supply, installation, testing and commissioning of the IT infrastructure at DC, DR to be hosted at preferred CSP's data center and installation , supply and commission of the LAN and WAN infrastructure at the NMDC project locations and HO along with support and maintenance for a period of 5 years from the date of Service acceptance by NMDC.

The overall Scope of Work (SoW) for the bidder to be appointed through this RFP includes the following but not limited to-

a) Supply, installation and configuration, testing and commissioning of compute, Network and Security infrastructure (hardware & software) such as Servers, Operating systems and databases etc.

b) Supply, installation, configuration, testing and commissioning of Storage Area Network with Enterprise Class Storage system

c) Configuration and integration of security components should be done as per the guidelines provided by NMDC IT policies.

d) DR setup not in the same seismic zone of DC site, which include the complete storage replication of DC in sync mode to achieve near Zero RPO.

e) Supply, installation, configuration, testing and commissioning of LAN and WAN infrastructure like Switches, Cables, Panels, Towers, etc.

f) Supply, installation, configuration, testing and commissioning of Security infrastructure like Next Generation Firewalls, Antivirus, DDOS, PIM, HIPS, IDAM, DAM, IPS/IDS, Log Servers, and Web Application Firewall etc.

g) Five years comprehensive maintenance and provisioning of services of all the Infrastructure and their components supplied as per BOQ, on 24x7x365 basis after successful execution and acceptance by NMDC LTD.

h) Implementation and commissioning of ITSM tools for Asset management, incident, problem and change management as part of the solution. Tool proposed should be leader in Gartner quadrant and key stakeholders from NMDC should have access to the dashboards on the tool.

Data Center and DR Co Location

NMDC Ltd. is rolling out SAP HANA application to improve its operational efficiency among other objectives.

To support deployment of this critical application and to ensure a good user experience of the application(s), it is intended to roll out a state-of-the-art network and computing infrastructure. Further, SAP S4HANA application is planned to be deployed in a Multi-Tenanted Data Centre (Co-Location), supported by a DR center. The Data Center should be in Hyderabad and the service provider should have his own building. SAP Users will access the SAP (and other) applications from

a) Head Office at Hyderabad
b) Mines (and township) at Kirandul, Bacheli, Panna and Donimalai (and Kumaraswamy)
c) Steel Plants at Jagdalpur and Paloncha
d) R&D, and, several Branch offices

.
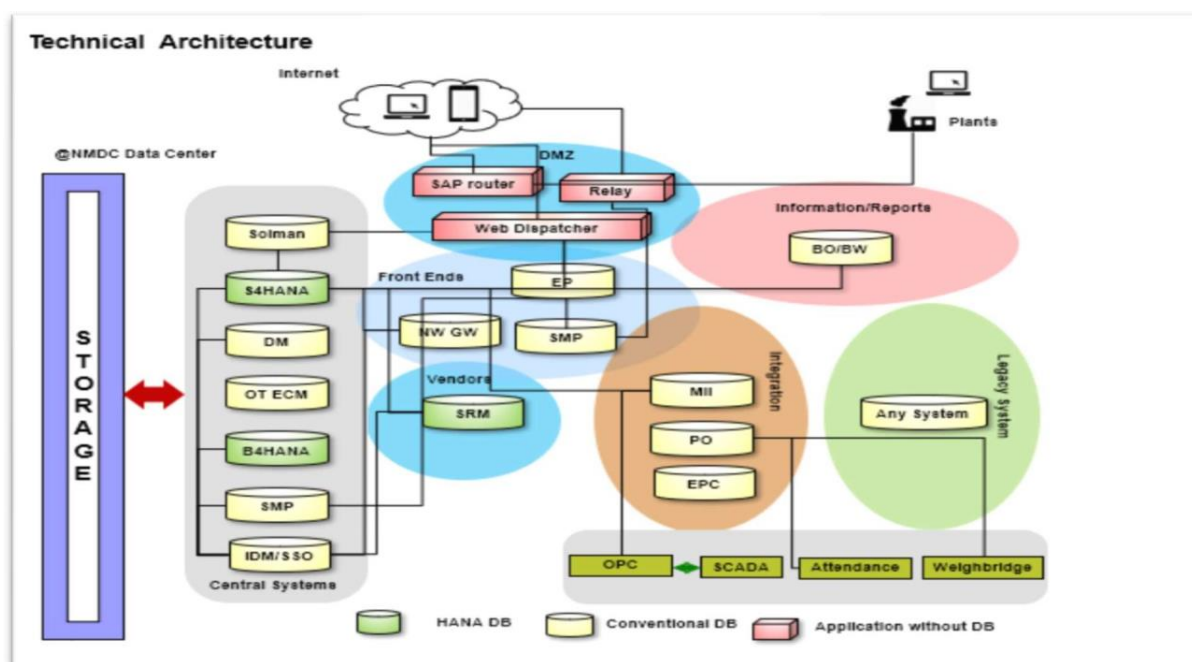
Fig: Application Landscape
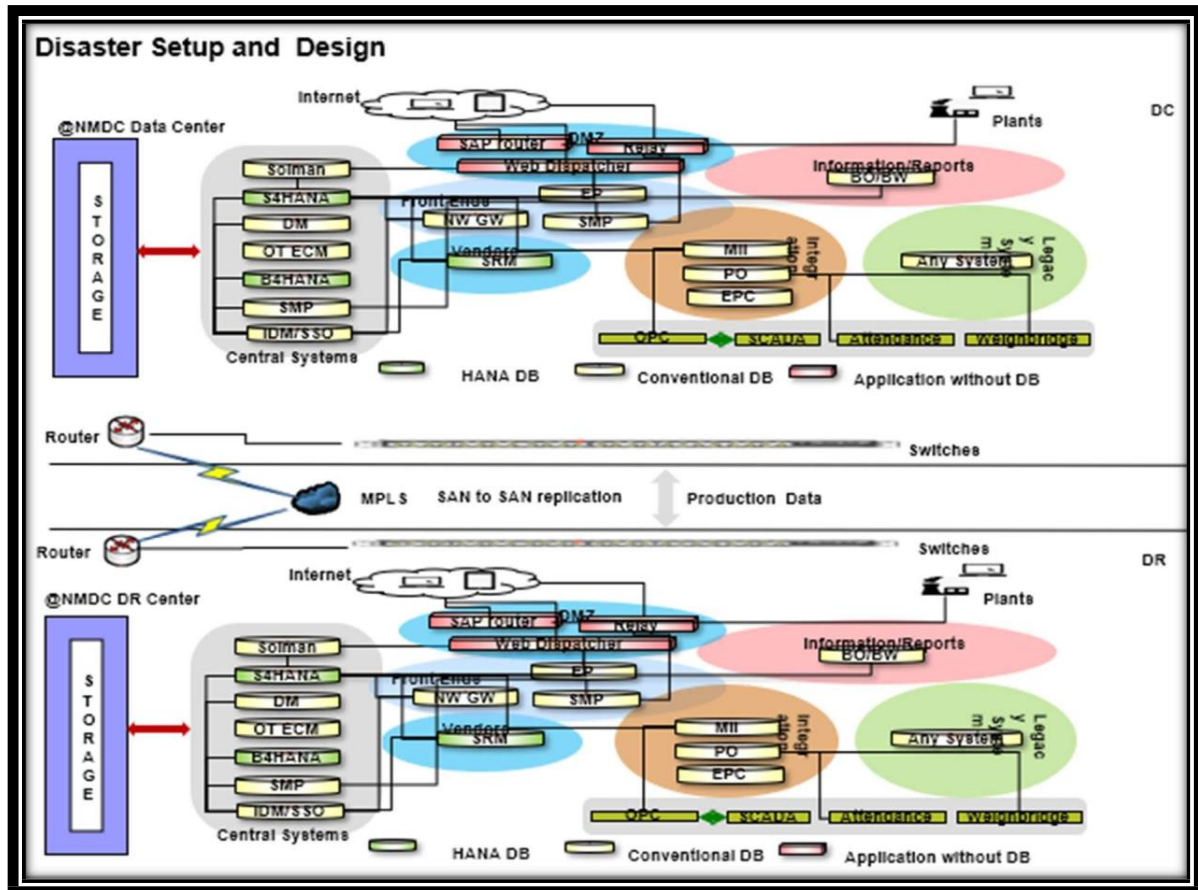
Fig : Technical Architecture for DC/DR Setup
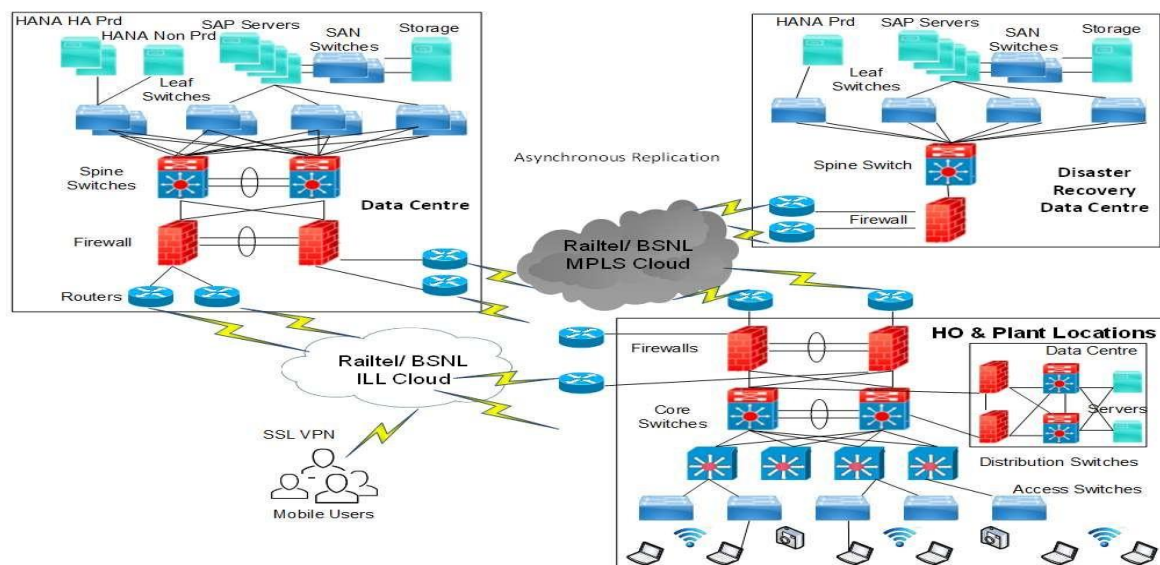
Fig : Intended LAN/WAN Setup for NMDC

NMDC will have a three-tier architecture as part of its SAP System landscape and will consist of

Development environment

Quality environment

Production environment

Disaster Recovery Environment

General Requirements Colocation & Managed Services

1. Data Centre Services for DC & DR to be in conformance with minimum Tier3 DC certification Norms.
2. Compliance process to the defined international standards and security guidelines such as ISO 27001, ISO 20000:1 for maintaining operations of cloud and ensuring privacy of NMDC data.
3. Ensuring Uptime and utilization of the cloud resources as per SLA's defined in this RFP.
4. In the event of a disaster at DC site, activation of services from the DR site is the responsibility of Implementation partner. Implementation partner shall develop appropriate policy, checklists in line with ISO 27001 & ISO 20000 framework for failover and fall back to the appropriate DR site. DR drills needs to be performed by Implementation partner half yearly to check disaster preparedness
5. DC & DR should be from same service provider and should not be in the same seismic zone.
6. Implementation partner shall conduct vulnerability and penetration test (from a third-party testing agency which may be CERT-IN empaneled) on the Cloud facility every 6 months and reports should be shared with ITI.
7. Implementation partner needs to update the system in response to any adverse findings in the report, without any additional cost to ITI.
8. Any required version/Software /Hardware upgrades, patch management etc. will be supported by the Implementation partner for the entire contract period at no extra cost to ITI.
9. Perform Due Diligence study and submit report for Migration of legacy applications not being covered under SAP data migration (e.g. Intranet Portal, Vigilance application etc.) at HO and Sites to DC & DR.
10. Perform Due Diligence Study and submit plan for Migration and support of legacy applications (e.g. HRMS/FAS/PMS/IMS/Payroll etc.) for historical reporting for statutory requirements.
11. Implementation partner shall submit the following reports on a regular basis. The following is only an indicative list of MIS reports that may be submitted to the ITI / NMDC.

Daily Reports

12. Summary of resolved, unresolved and escalated issues / complaints Log of backup and restoration undertaken

Weekly Reports

13. Summary of systems rebooted.
14. Summary of issues / complaints logged with the OEMs.
15. Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.
16. Hypervisor patch update status of all servers including the Virtual Machines running

Monthly Reports

17. Component wise server as well as Virtual machines availability and resource utilization
18. Consolidated SLA / Non- conformance report.
19. Summary of component wise uptime.
20. Log of preventive / scheduled maintenance undertaken
21. Log of break-fix maintenance undertaken.
22. All relevant reports required for calculation of SLAs
23. Logs of any Security Breaches

Quarterly Reports

24. Consolidated component-wise availability and resource utilization
25. All relevant reports required for calculation of SLAs
26. The MIS reports shall be in-line with the SLAs and the same shall be scrutinized by the ITI / NMDC.

Manpower Deployment List

A list needs to be provided with resources who will be deployed on the project along with the roles and responsibilities of each resource.

Resource Deployment List

List and number of all cloud-based resources (including but not limited to servers (VMs), storage, network components and software components) other than manpower that may be required.

Progress Monitoring Plan and Reporting Plan

Detailed Daily, Weekly, Monthly Progress Report formats along with issue escalation format. The format will be approved by ITI / NMDC before start of the project.

Standard Operating Procedures

Detailed procedures for monitoring and raising the incident on the Cloud site.

Risk Mitigation Plan

List of all possible risks and methods to mitigate them.

Escalation Matrix & Incident Management

A detailed list of key contact persons with contact details with escalation hierarchy for resolution of issues and problems. This must be via an Incident Management system.

LAN/WAN Infrastructure

NMDC is planning to revamp its existing LAN and WAN Infrastructure, to make it more robust and to be able to provide the backbone support for its ERP and Other Digital initiative as per its Roadmap.

In accordance with the above, NMDC is proposing to make the changes to its existing landscape at it project location as below

1. New 3-tier (Core, Distribution & Access) hierarchical star LAN network infrastructure is being proposed for
   a. Kirandul,
   b. Bacheli, and
   c. Donimalai
2. New 2 layer – Core and Access for
   d. Panna
   e. Paloncha

   a. LAN for the Jagdalpur plant is not considered to be part of the Scope of this RFP.
   b. Change to the Active and Passive devices (like Switches, Routers) are being considered for Branch offices, corporate office.
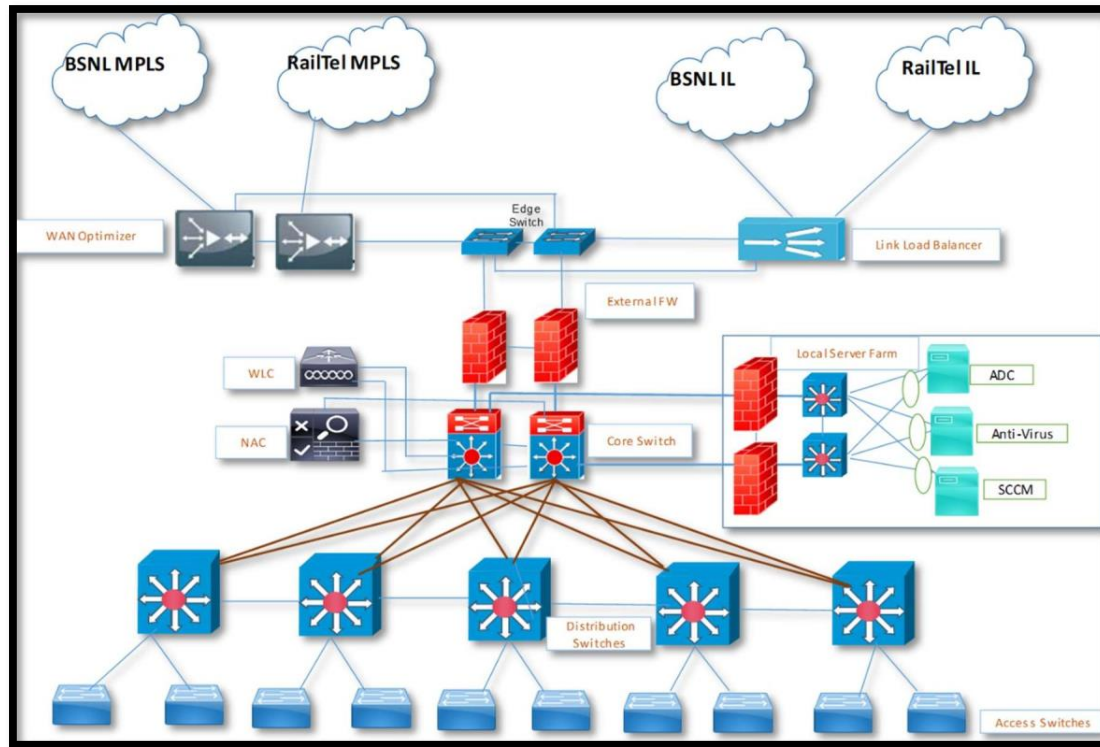
Fig : Proposed LAN Network Diagram

General Requirements for the LAN Infrastructure

1. Implementation partner Needs to provide the proposed technical architecture document for the LAN and WAN Setup which should cover in detail and at Minimum following sections

   a. Detailed Project Plan for Design, Supply, Installation, Testing and Commissioning of LAN Infrastructure project site wise.

   b. Network segmentation strategy, Outdoor Wi-Fi installation strategy in plant and mines, security architecture for PLC/SCADA systems.

   c. Cabling methodology, EMS, NAC and WIFI (compliance to IEEE 802.11ac standards)

   d. Service adherence, compliance, monitoring and reporting details.

   e. Security Solutions proposed including Antivirus, certificates, fire wall, VAPT testing etc.

   f. Reliability and scalability of solution, open architecture and availability of the business-critical applications on High availability.

   g. Data Encryption standards (for Data at rest and In-transit).

   h. Patch management, upgrades frequency, Active Directory service management etc.

   i. Wan optimization and load balancing strategy

   j. Help desk (onsite, off shore, OEM support etc.) SNMP, NMS monitoring, management and incident reporting.

General Requirements of WAN Infrastructure

1. Implementation partner Needs to provide the proposed technical architecture document for the LAN and WAN Setup which should cover in detail and at Minimum following sections
   a. Detailed Project Plan for Design, Supply, Installation, Testing and Commissioning of WAN Infrastructure project site wise.
   b. Network segmentation strategy, Outdoor Wi-Fi installation strategy in plant and mines, Uptime, availability, throughput, latency, packet losses etc.
   c. Design of the MPLS network, sizing, link management and backup link solutions for critical applications and users.
   d. Help desk, SLA management, monitoring, reporting

Geographical Scope

The following provides the details of the Geographical coverage for this project. The details of NMDC's operational offices and its project locations have been provided and it is expected that the Service provider covers all these locations as part of the solution that they provide.

Project Locations	Locations	State
	1. Bacheli	Chhattisgarh
	2. Kirandul	Chhattisgarh
	3. Donimalai	Karnataka
	4. Kumaraswamy	Karnataka
	5. Panna	Madhya Pradesh
	6. Pellet Plant - Donimalai	Karnataka
	7. SIU – Paloncha	Telangana

Head Office	1. Corporate HO – Hyderabad	Telangana
Regional Offices	1. Vizag	Andhra Pradesh
	2. Chennai	Tamil Nadu
	3. Mumbai	Maharashtra
	4. Kolkata	West Bengal
	5. GEC Raipur	Chhattisgarh
	6. R&D Centre – Hyderabad	Telangana
	7. Delhi Office	Delhi

General Requirements

1. Implementation partner Needs to provide the proposed technical architecture document for the Support and Help desk services for all locations in detail and at minimum covering
   a. Help desk model (onsite, off shore, OEM support etc.) SNMP, NMS monitoring, management and incident reporting.
   b. Service adherence, compliance, monitoring and reporting details.
   c. Resource deployment plan
   d. Help desk Tools to be used

2 Section-A

Kirandul Iron Ore Mine

Network Design Single Line Diagram
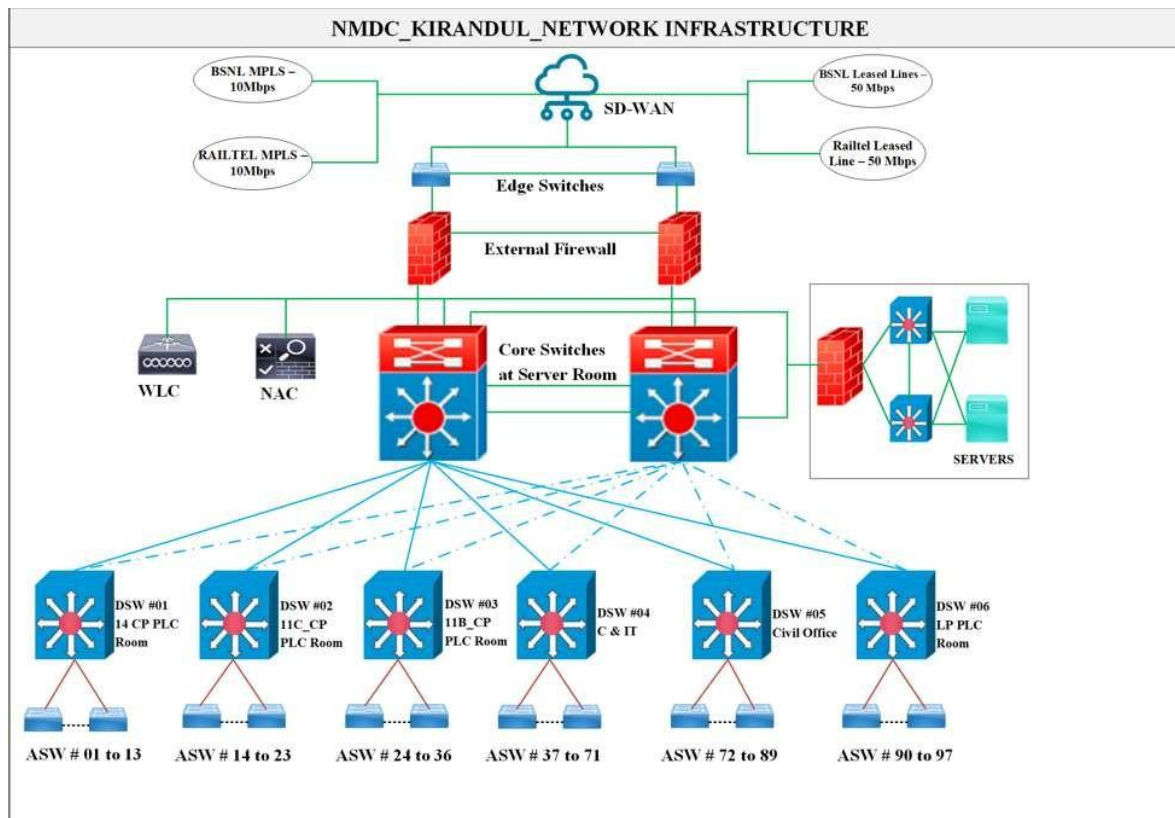
Fig 1 Kirandul Single Line Diagram
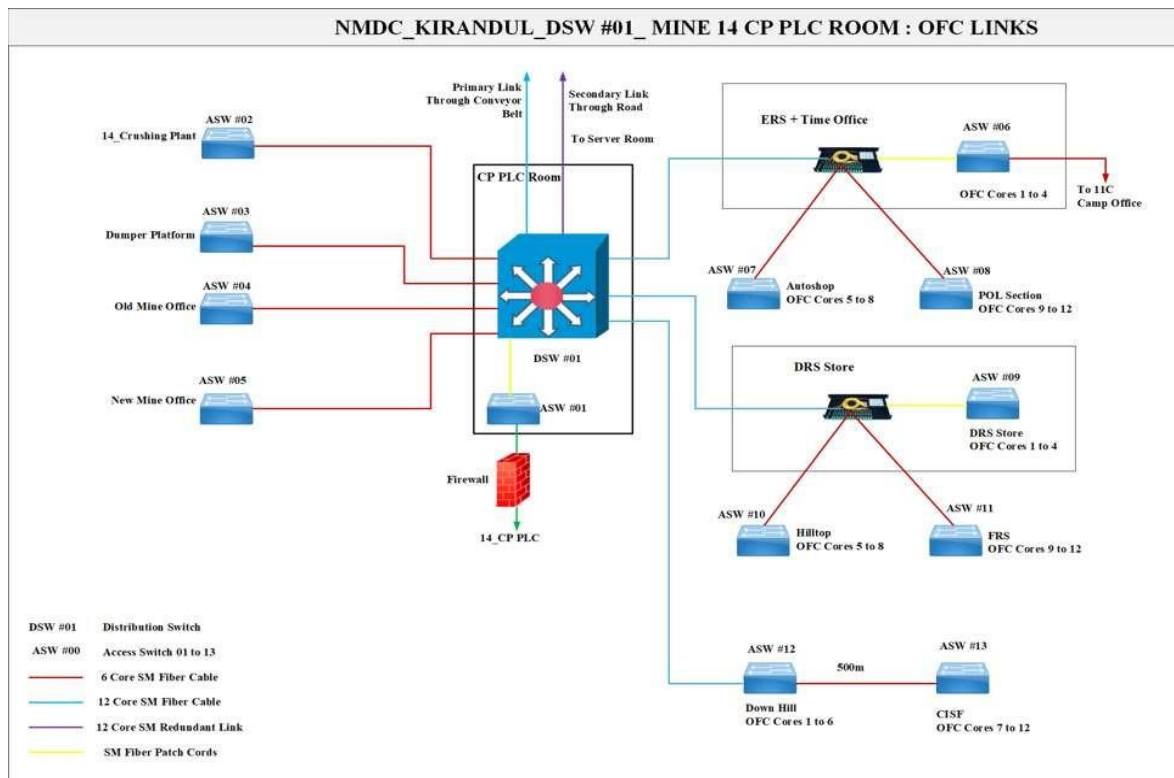
Fig 2 Kirandul Distribution Switch#1 Network Diagram
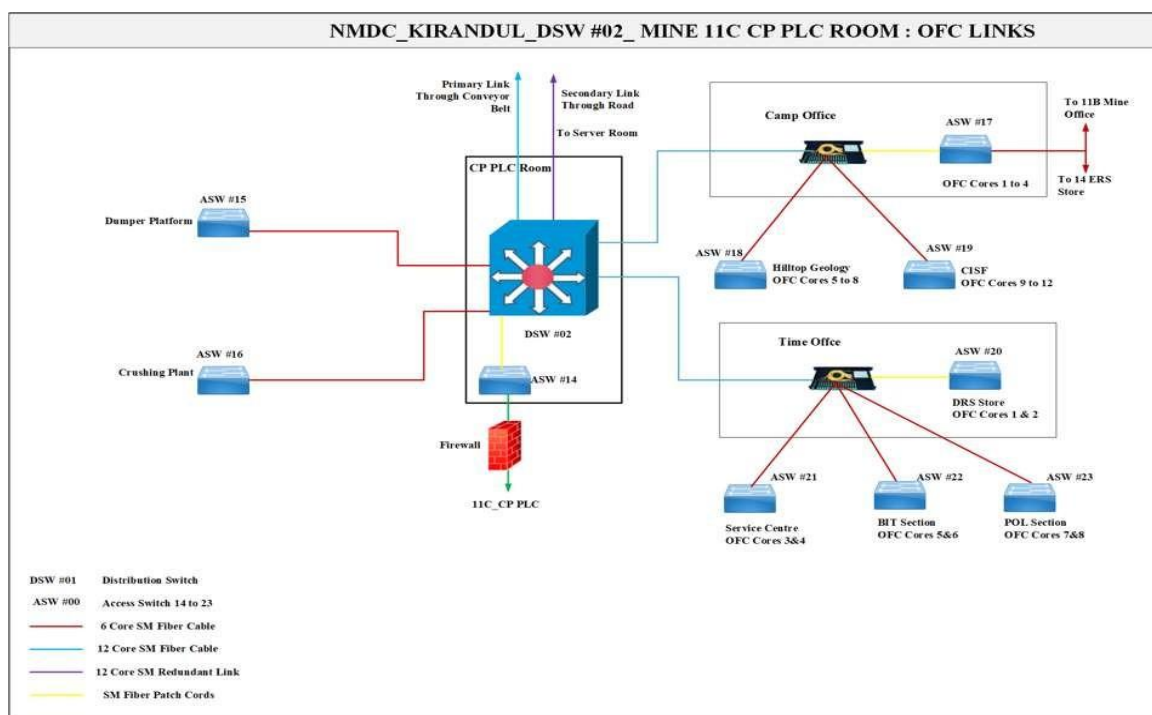
Fig 3 Kirandul Distribution Switch#2 Network Diagram
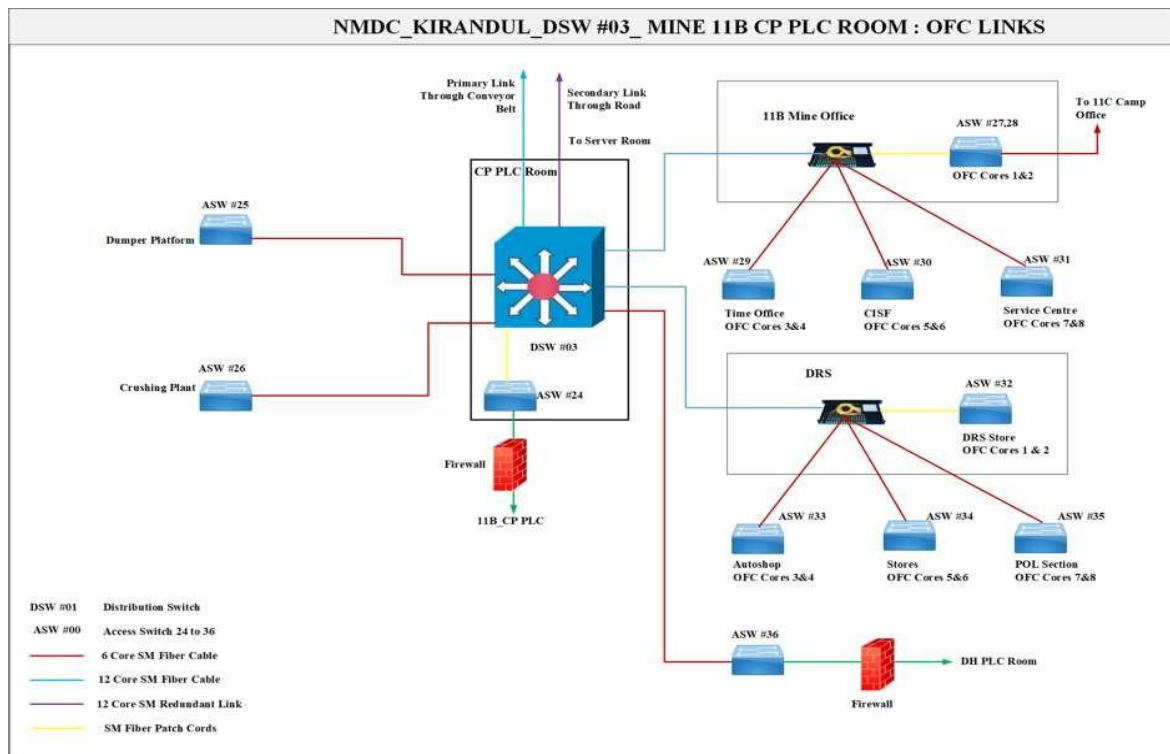
Fig 4 Kirandul Distribution Switch#3 Network Diagram
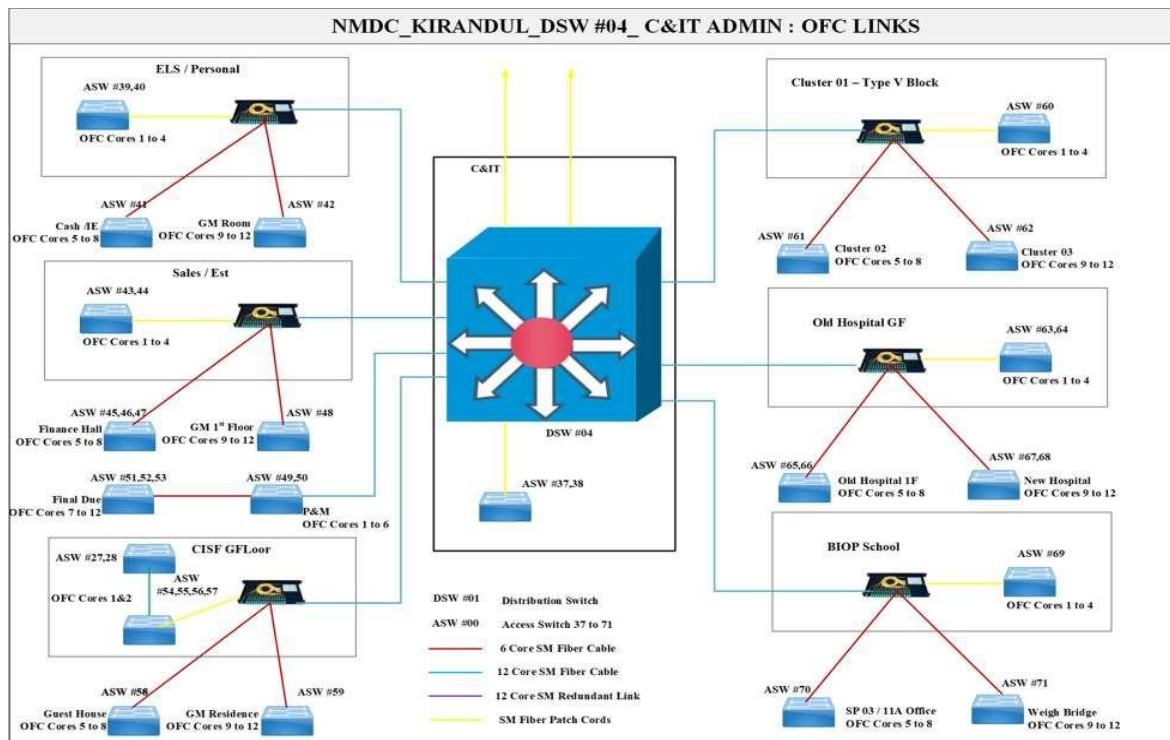
Fig 5 Kirandul Distribution Switch#4 Network Diagram
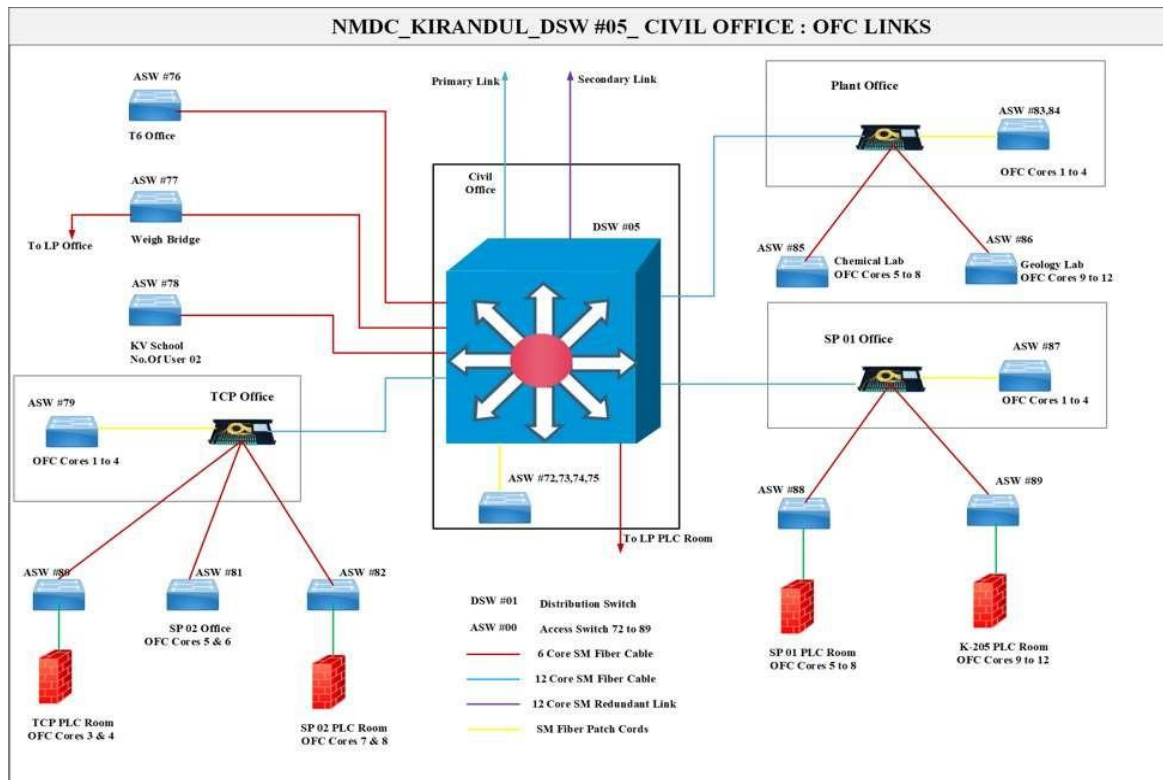
Fig 6 Kirandul Distribution Switch#5 Network Diagram
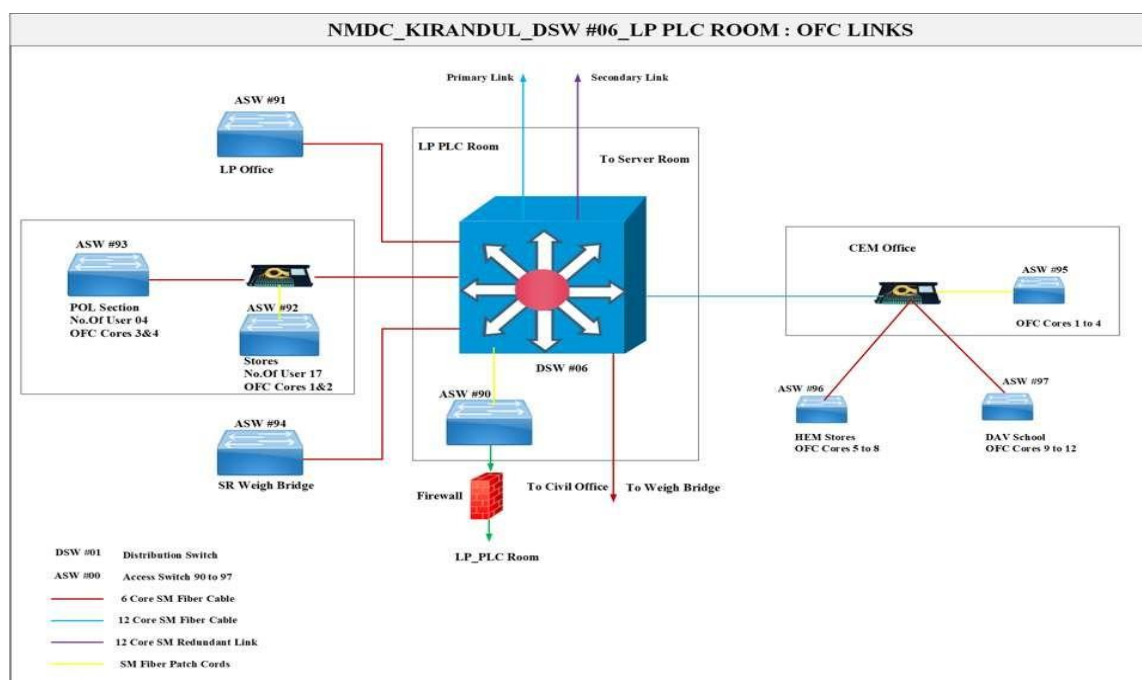
Fig 7 Kirandul Distribution Switch#6 Network Diagram

Redundant OFC Links

- 14 ERS to 11C Camp Office
- 11C Camp Office to 11B Mine Office
- Old Hospital to Weigh Bridge
- LP PLC Room to Civil Office
- LP PLC Room to Weigh Bridge

Outdoor Wi-Fi for Mining Area

- Provide outdoor coverage for gathering data from devices on-board moving vehicles.
- Connectivity on Wi-Fi / unlicensed bands preferred.
- At each mine, we propose 2 Wi-Fi zones for data collection
  - One covering the vehicles inside the mine
    - Backhaul to be planned on P2P radio links
    - One covering the vehicles near the crusher plant
      - Backhaul is on optical Fiber
  - The idea of providing the 2nd Wi-Fi zone at Crusher plant is to make sure data is collected from each vehicle at least once during a trip

Kirandul: Has 3 mines

Mine 14, Mine 11B, Mine 11C

Kirandul 14 Coverage Area

Fig 8 Kirandul Mine 14 Coverage Area

Kirandul 14 Locations for Root Access Points

Fig 9 Kirandul 14 Root Access Point Locations

Kirandul 14 Wireless PTP backhaul Link for Root AP # 1

Fig 10 Kirandul 14 Wireless P2P Backhaul

Kirandul 14 Existing Fiber Optic Link to Crusher Plant Backhaul for Root AP # 2

Fig 11 Kirandul 14 Crusher Plant Backhaul

Kirandul 14 - Summary

- o Total Wi-Fi Hotspot zones: 2
- o Number of PTP links: 1
- o Root AP # 1 to be connected on Wireless Backhaul link
    - o Approximate link distance 550 M
- o Root AP # 2 is having OFC connectivity (Crusher Plant)

Kirandul 11B Coverage Area

Fig 12 Kirandul 11B Coverage Area

Kirandul 11B - Locations for Root Access Points

Fig 13 Kirandul 11B Root Access Point Locations Kirandul 11B

– Wireless Link for Root AP # 1 Wireless PTP backhaul

Fig 14 Kirandul 11B Wireless PTP Backhaul

Kirandul 11B - Fiber Optic backhaul Available at Location Root AP # 2

Fig 15 Kirandul 11B Fiber Optic Backhaul

Kirandul 11B - Summary

- Total Wi-Fi Zones: 2
- Number of PTP links: 1
- Root AP # 1 to be connected on Wireless Backhaul link
    - Approximate link distance 910 M
- Root AP # 2 is having OFC backhaul connectivity

Kirandul 11C Coverage Area

Fig 16 Kirandul 11C Coverage Area

Kirandul 11C – Locations for Wi-Fi Zones

Fig 17 Kirandul 11C Wi-Fi Zones

Kirandul 11C - Wireless Link for Root AP # 1 & # 3

Fig 18 Kirandul 11C Wireless Link

Kirandul 11C – Fiber Optic backhaul Available at Location Root AP # 2

Fig 19 Kirandul 11C Fiber Optic Backhaul

Kirandul 11C - Summary

- o Total Wi-Fi Zones: 3
- o Number of PTP links: 2
- o Location 1 & 3 to be connected on Wireless Backhaul link
    - o Link 1 distance 1180 M
    - o Link 3 distance 830 M
- o Location 2 is having OFC backhaul connectivity

Bacheli Iron Ore Mine

Network Design Single Line Diagram
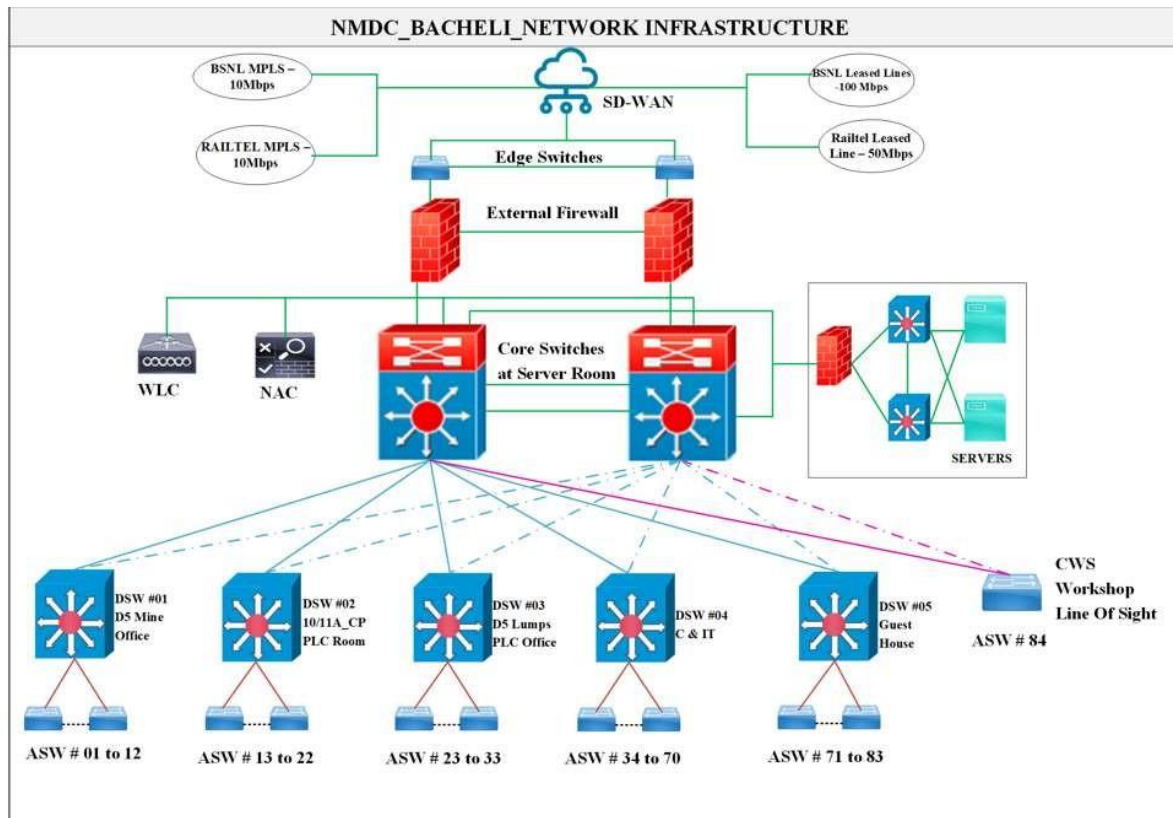
Fig 20 Bacheli Single Line Diagram
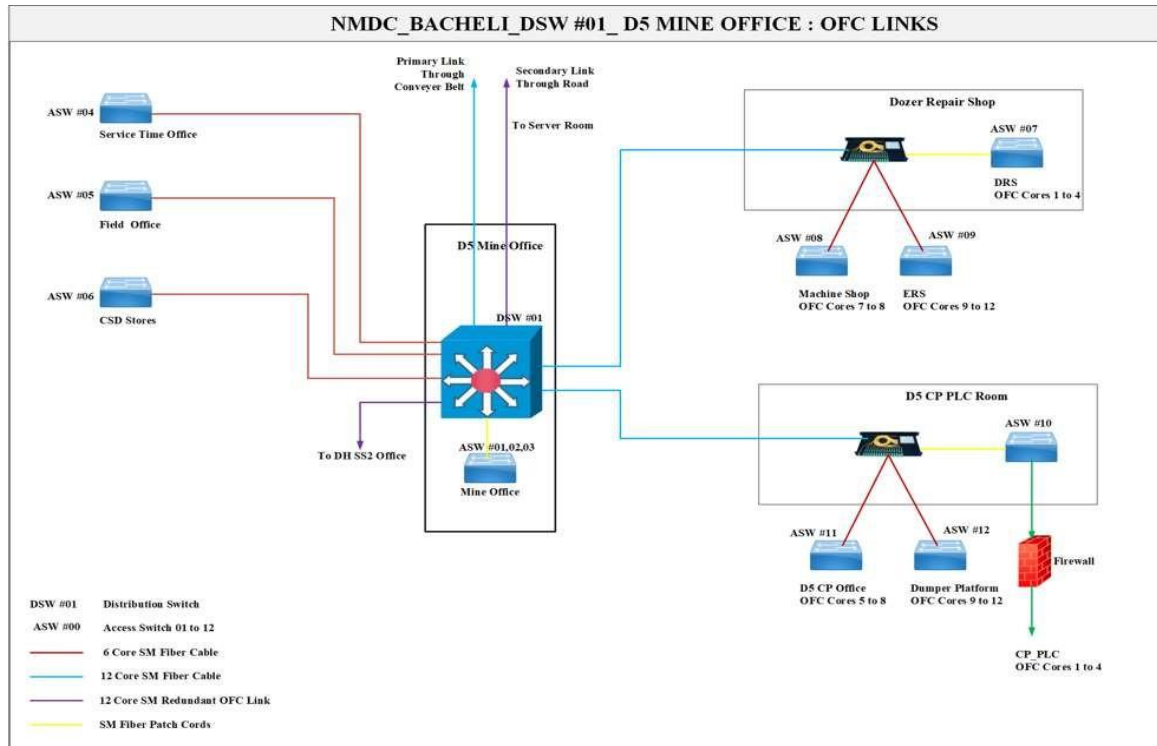
Fig 21 Bacheli Distribution Switch#1 Network Diagram
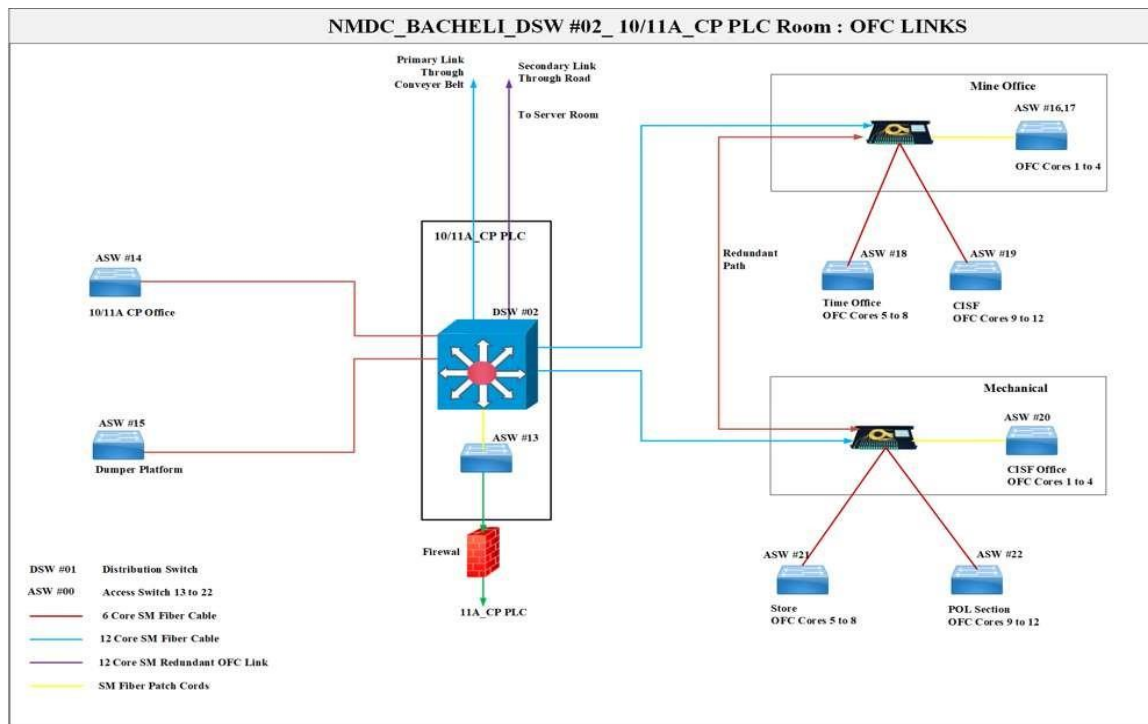
Fig 22 Bacheli Distribution Switch#2 Network Diagram
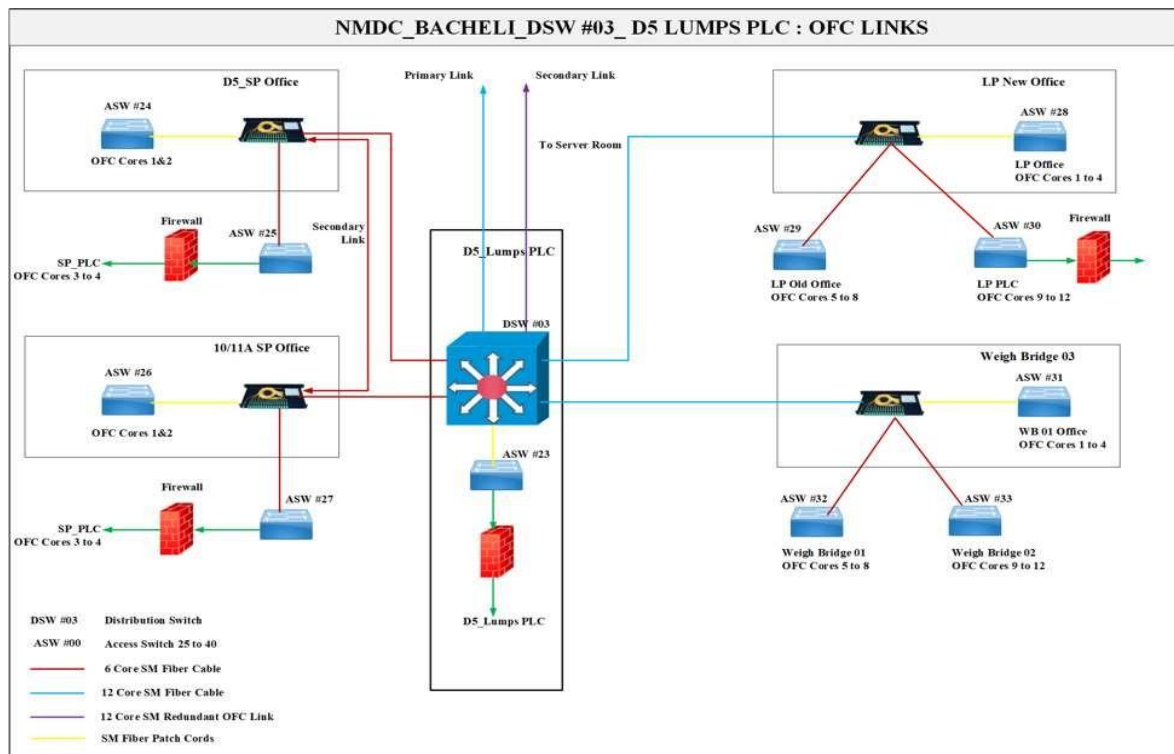
Fig 23 Bacheli Distribution Switch#3 Network Diagram
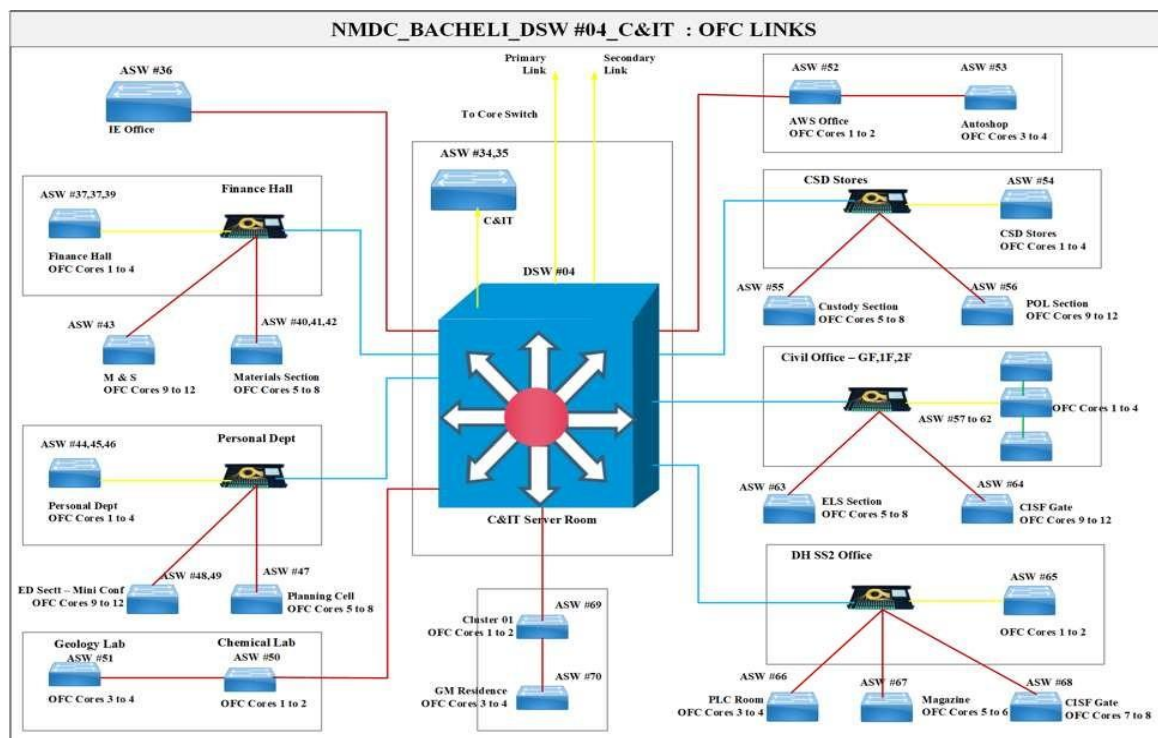
Fig 24 Bacheli Distribution Switch#4 Network Diagram
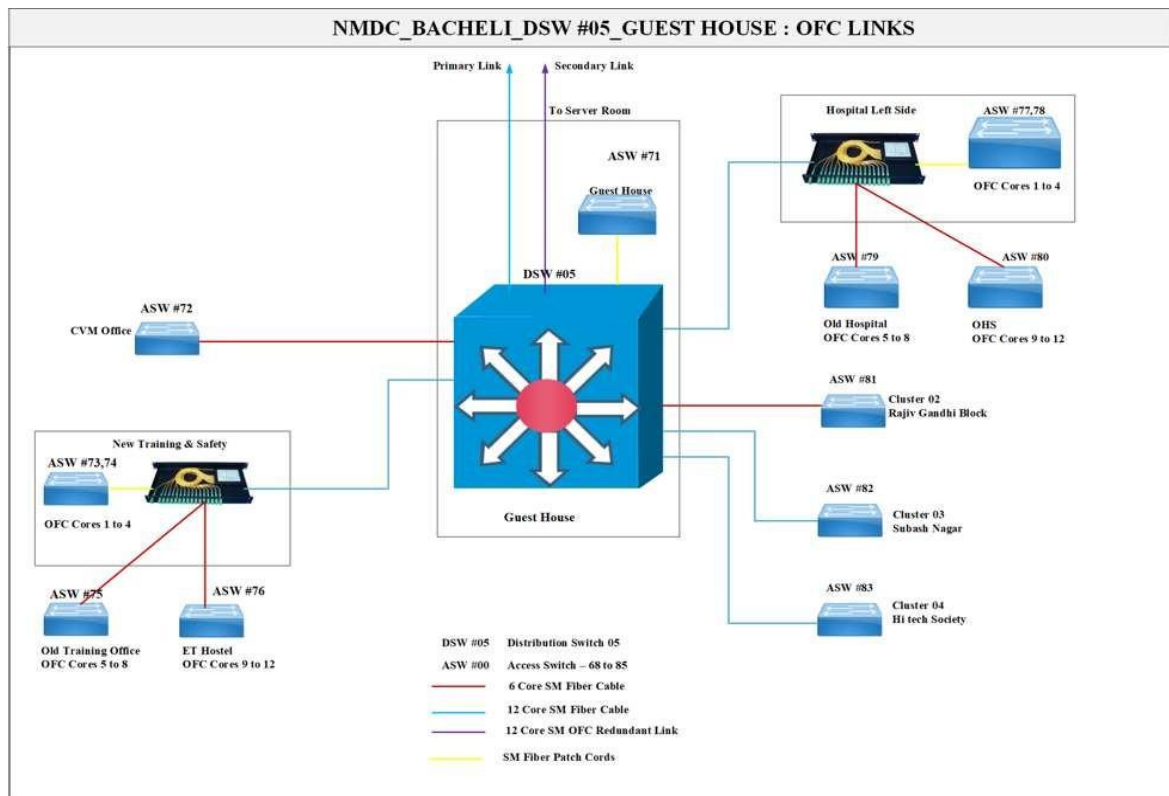
Fig 25 Bacheli Distribution Switch#5 Network Diagram
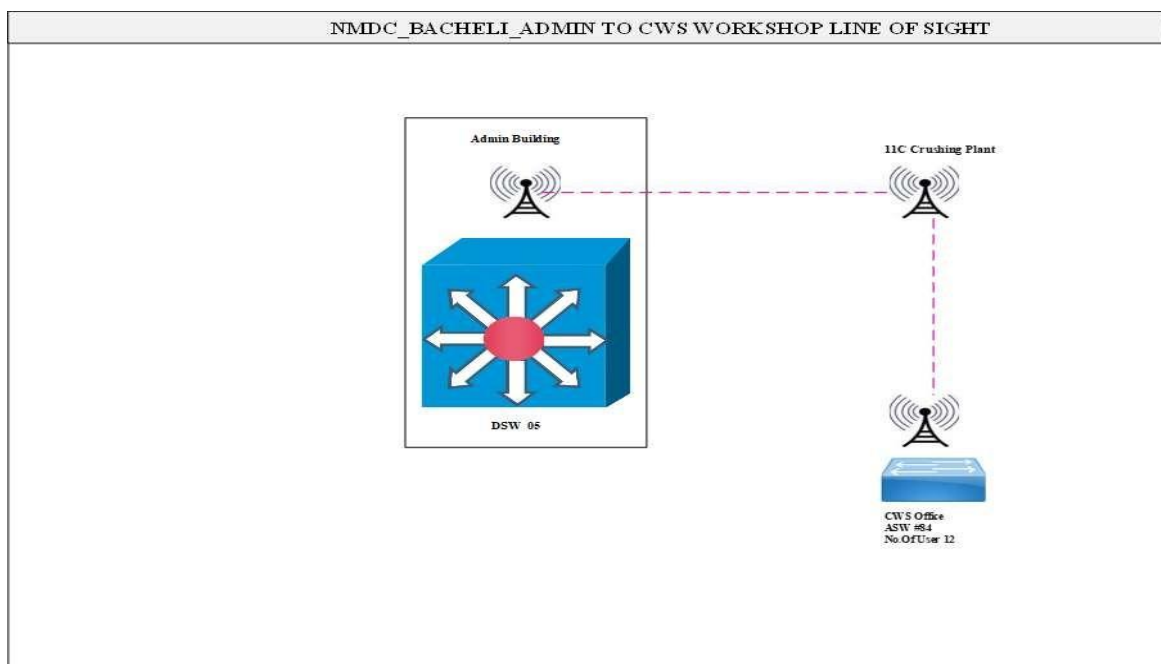
Fig 26 Bacheli Admin to CWS LoS
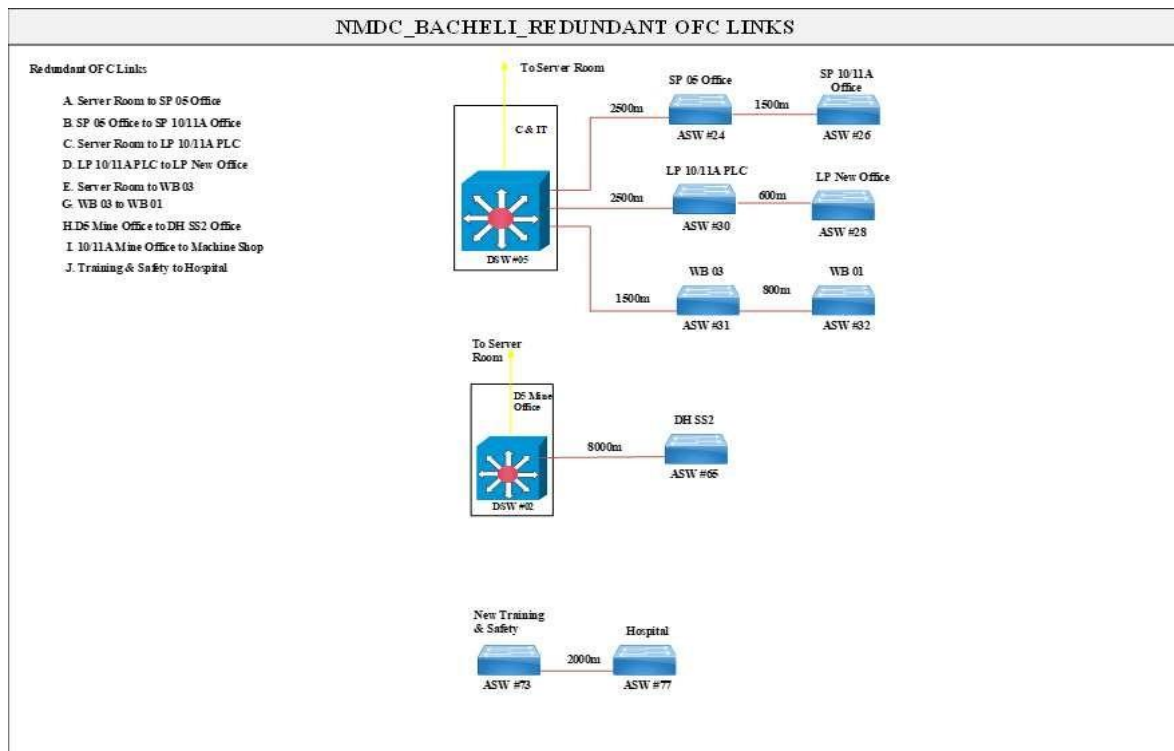
Fig 27 Bacheli OFC Redundant Links

Fig 28 Bacheli Admin to CWS LoS

Outdoor Wi-Fi for Mining Area

- Provide outdoor coverage for gathering data from devices on-board moving vehicles.
- Connectivity on Wi-Fi / unlicensed bands preferred.
- At each mine, we propose 2 Wi-Fi zones for data collection
  - One covering the vehicles inside the mine
    - Backhaul to be planned on P2P radio links
  - One covering the vehicles near the crusher plant
    - Backhaul is on optical Fiber
  - The idea of providing the 2nd Wi-Fi zone at Crusher plant is to make sure data is collected from each vehicle at least once during a trip

Bacheli: Has 2 mines
Mine D5, Mine 10/11A Bacheli

D5 – Coverage Area

Fig 29 Bacheli D5 Coverage Area

Bacheli D5 – Locations for Wi-Fi Zones

Fig 30 Bacheli D5 Wi-Fi Zone Locations

Bacheli D5 – Wireless Link for Root AP # 1 & # 2

Fig 31 Bacheli D5 Wi-Fi Links

Bacheli D5 - Summary

- o   Total Wi-Fi Zones: 2
- o   Number of PTP links: 2
- o   Location 1 & 2 to be connected on Wireless Backhaul link
    - o   Link 1 distance 650 M
    - o   Link 2 distance 590 M

Bacheli 10/11A Coverage Area

Fig 32 Bacheli 10/11A Coverage Area

Bacheli 10/11A – Locations for Wi-Fi Zones
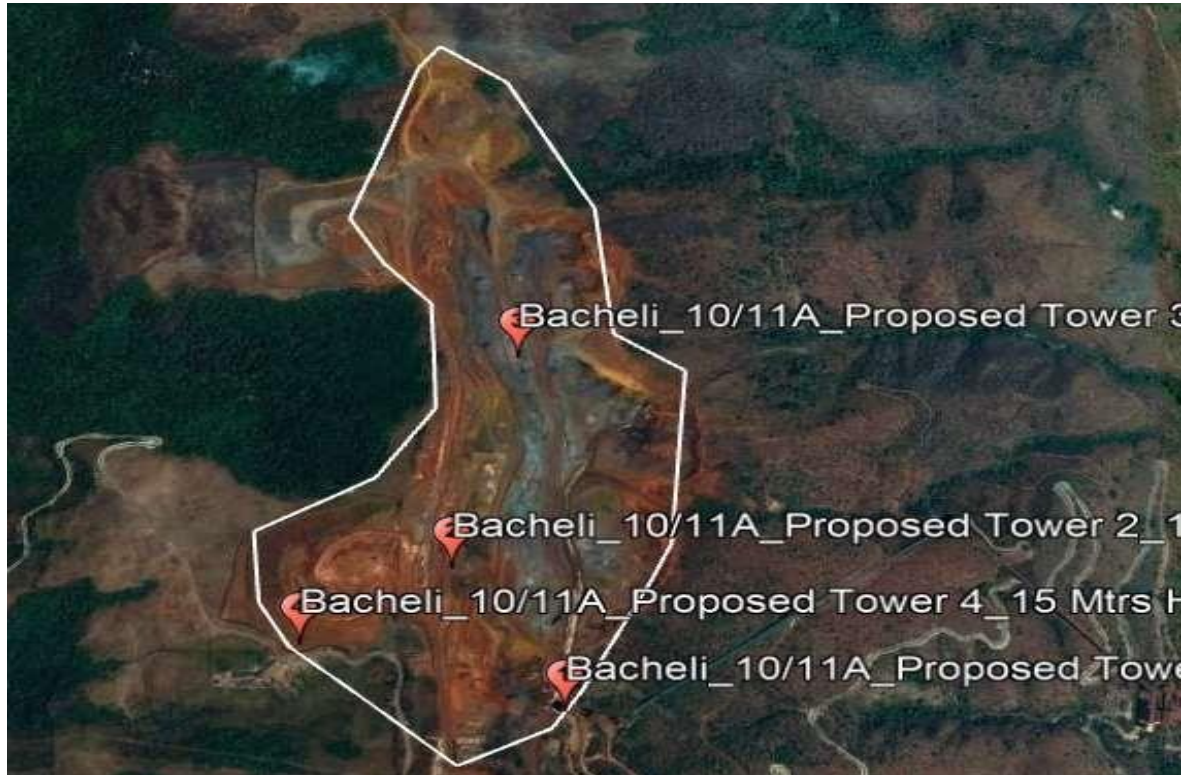
Fig 33 Bacheli 10/11A Wi-Fi Zones

Bacheli 10/11A – Fiber Optic backhaul Link Available at Root AP # 1

Fig 34 Bacheli 10/11A Fiber Optic Backhaul

Bacheli 10/11A – Wireless Link for Root AP # 2 from Root AP #1

Fig 35 Bacheli 10/11A Wireless Link for AP#2

Bacheli 10/11A – Wireless Link for Root AP # 3 from Root AP #1

Fig 36 Bacheli 10/11A Wireless Link for AP#3

Bacheli 10/11A – Wireless backhaul Link for Root AP # 4 from Root AP # 1

Fig 37 Bacheli 10/11A Wireless Link for AP#4

Bacheli 10/11A – Summary

- o Total Wi-Fi Zones: 4
- o Number of PTP links: 3
- o Root AP # 2, # 3 & # 4 to be connected on Wireless Backhaul link
    - o Link 2 distance 420 M
    - o Link 3 distance 890 M
    - o Link 4 distance 520 M
- o Root AP # 1 is having OFC backhaul connectivity

Donimalai Iron Ore Mine

Network Design Single Line Diagram
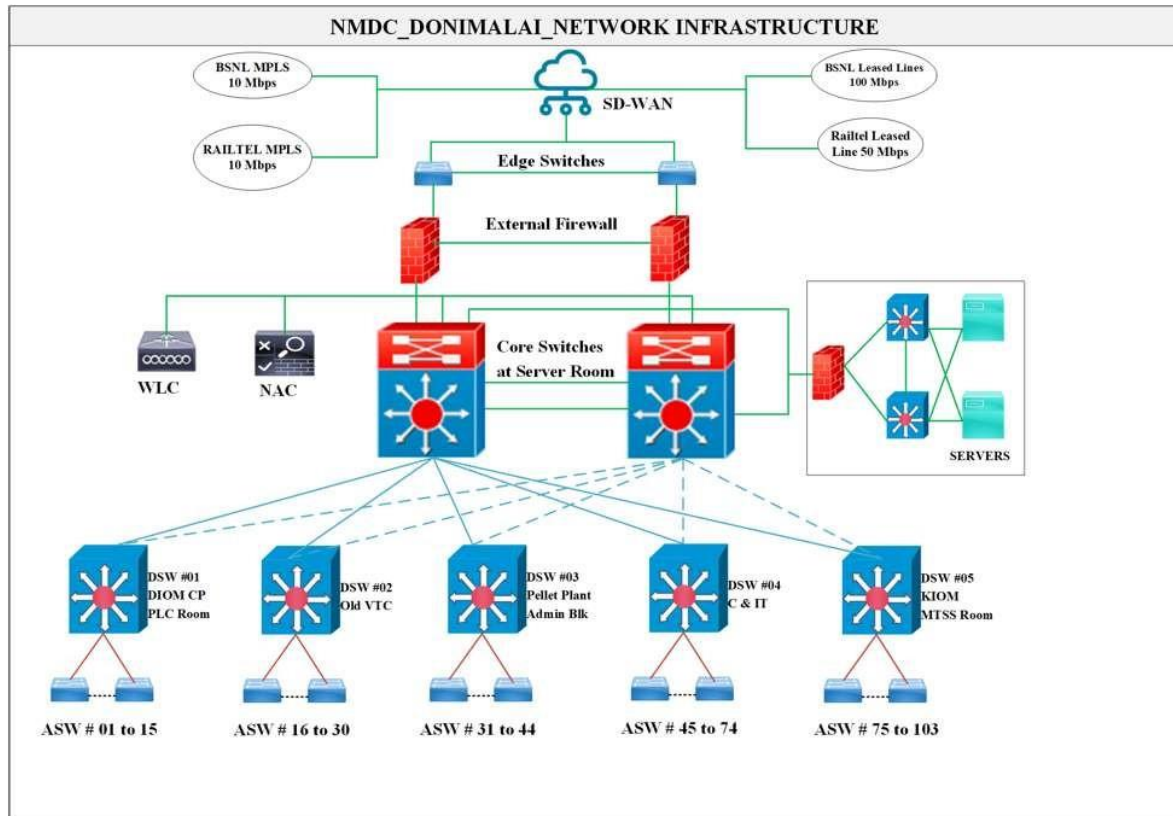

Fig 38 Donimalai Single Line Diagram
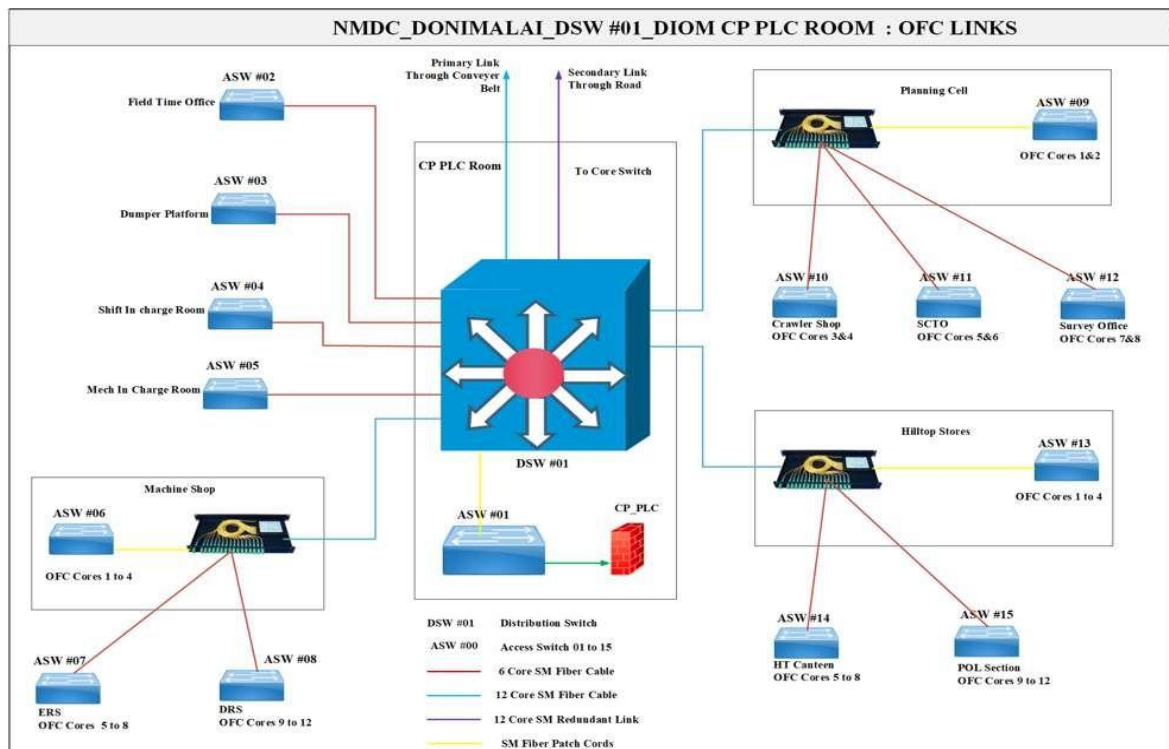
**Fig 39 Donimalai Distribution Switch#1 Network Diagram**
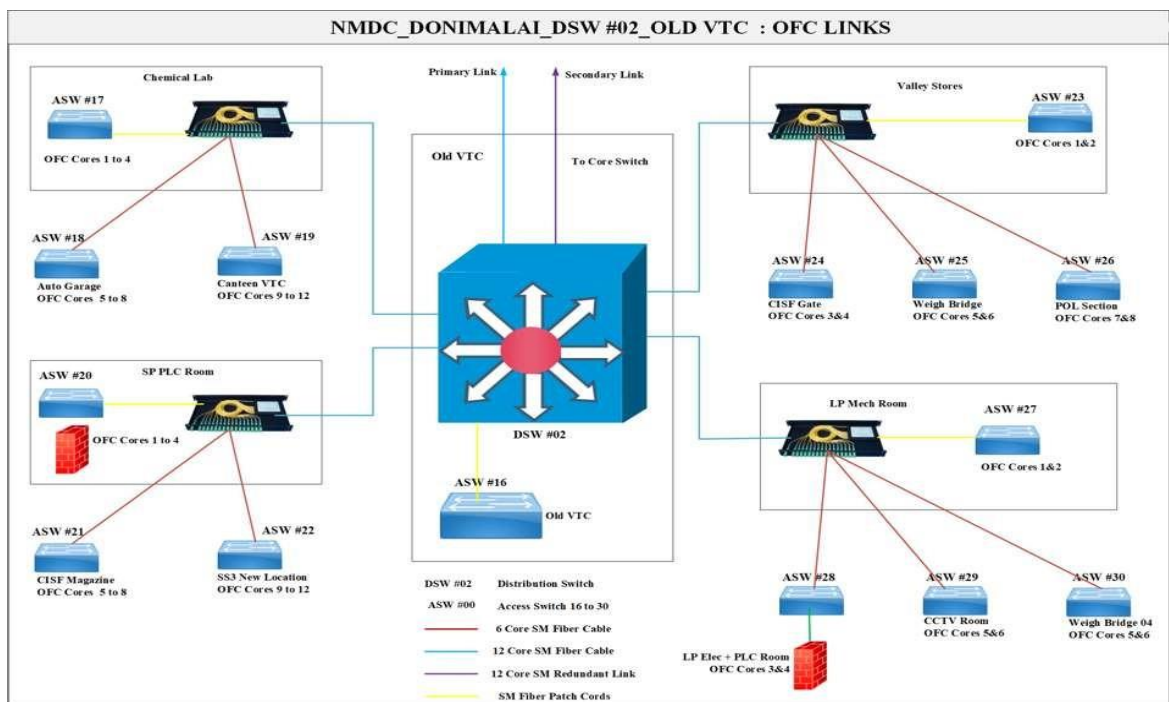
Fig 40 Donimalai Distribution Switch#2 Network Diagram
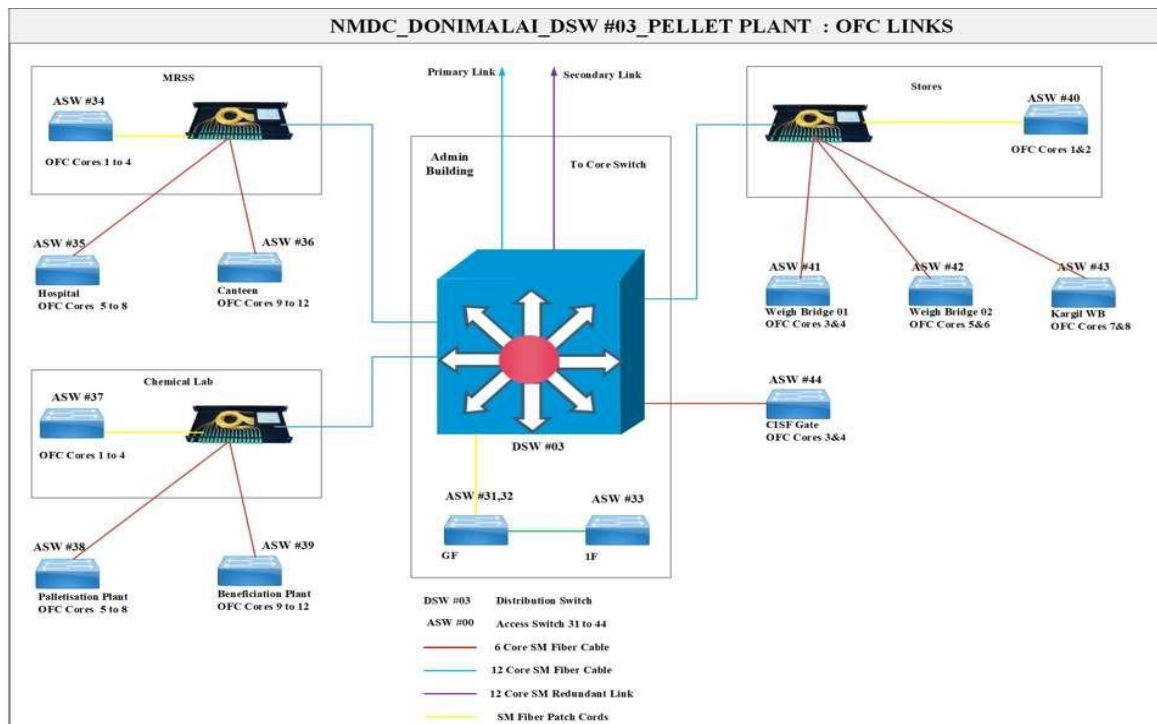
Fig 41 Donimalai Distribution Switch#3 Network Diagram
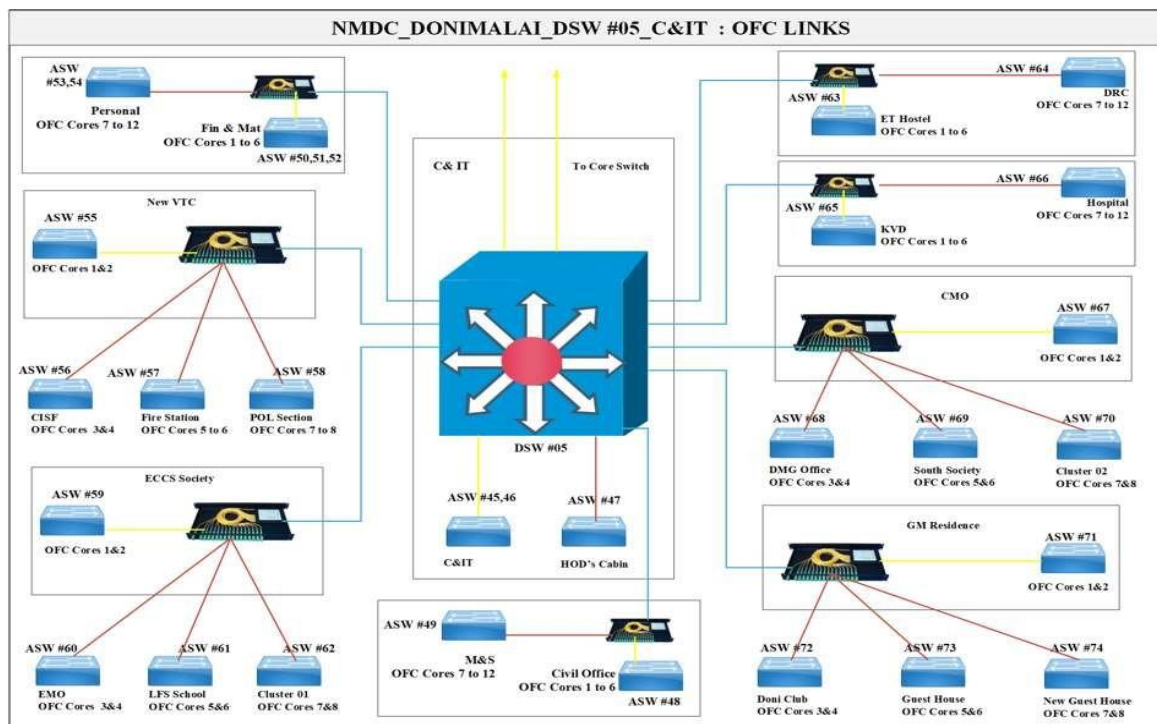
Fig 42 Donimalai Distribution Switch#5 Network Diagram
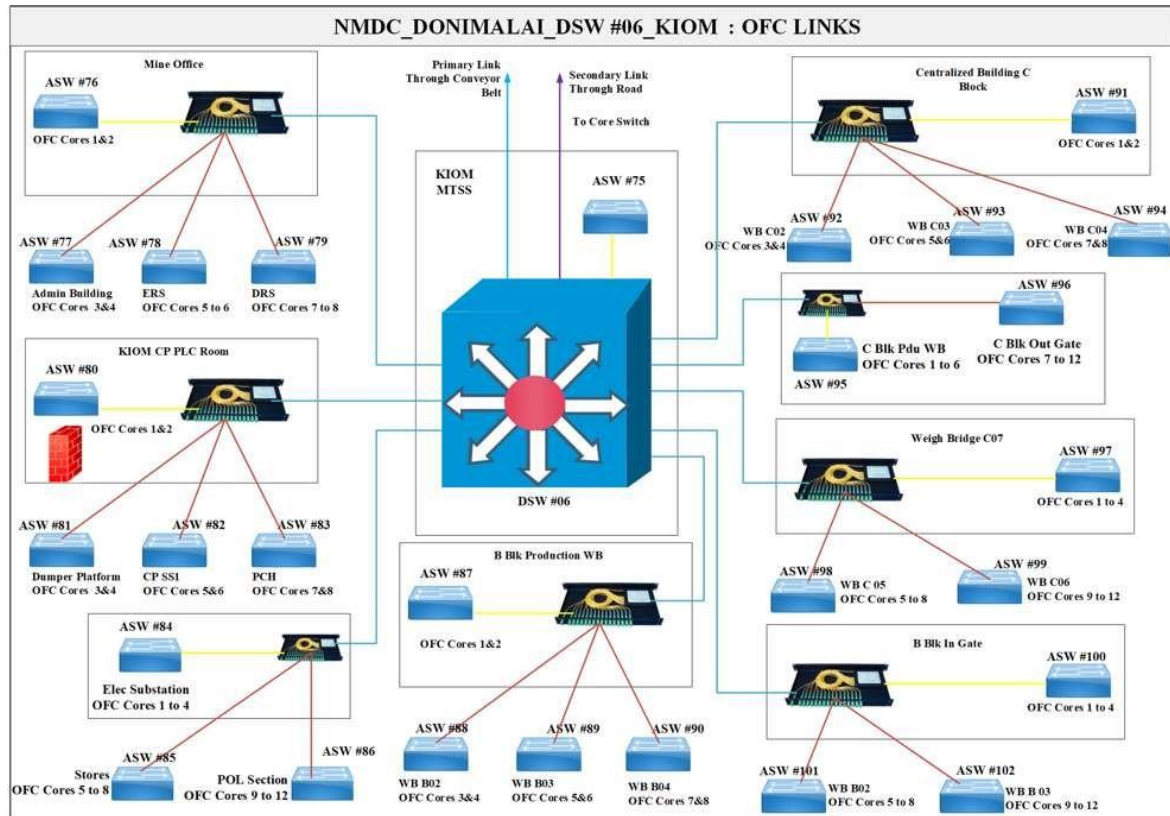
Fig 43 Donimalai Distribution Switch#6 Network Diagram

Line of Sight Details

DIOM CP PLC Room to Planning Cell Server

Room to SP PLC Room (SCADA) KIOM

MTSS Room to KIOM PLC Room

Pellet Plant Admin Building to LP Mech Room

Outdoor Wi-Fi for Mining Area

- Provide outdoor coverage for gathering data from devices on-board moving vehicles.
- Connectivity on Wi-Fi / unlicensed bands preferred.
- At each mine, we propose 2 Wi-Fi zones for data collection
  - One covering the vehicles inside the mine
    - Backhaul to be planned on P2P radio links

- One covering the vehicles near the crusher plant
  - Backhaul is on optical Fiber
- The idea of providing the 2nd Wi-Fi zone at Crusher plant is to make sure data is collected from each vehicle at least once during a trip

Donimalai: Has 1 mine **Kumaraswamy:**

Has 2 mines **Kumaraswamy_1,**

Kumaraswamy_2

Donimalai Coverage Area

Fig 44 Donimalai Coverage Area

Donimalai – Proposed Locations for Wi-Fi Zones

Fig 45 Donimalai Wi-Fi Zones

Donimalai – Fiber Optic backhaul Link Available at Root AP # 1

Fig 46 Donimalai Fiber Optic Backhaul

Donimalai – Proposed Wireless backhaul Link for Root AP # 2 from Root AP # 1

Fig 47 Donimalai Wireless Link for AP#2

Donimalai – Proposed Wireless backhaul Link for Root AP # 3 from Root AP # 2

Fig 48 Donimalai Wireless Link for AP#3

Donimalai – Proposed Wireless backhaul Link for Root AP # 4 from Root AP #3

Fig 49 Donimalai Wireless Link for AP#4

Donimalai – Proposed Wireless backhaul Link for Root AP #5 from Root AP#4

Fig 50 Donimalai Wireless Link for AP#5

Donimalai Summary

- o Total Wi-Fi zones: 5
- o Number of PTP links: 4
- o Root AP #2, #3, #4 & #5 to be connected on Wireless Backhaul link on daisy chain
  - o Link 2 distance 1110 M
  - o Link 3 distance 940 M (To be connected from Location 2)
  - o Link 4 distance 840 M (To be connected from Location 3)
  - o Link 5 distance 750 M (To be connected from Location 4)
- o Root AP # 1 is having OFC backhaul connectivity

Kumarswamy_1 – Coverage Area

Fig 51 Kumarswamy_1 Coverage Area

Kumarswamy_1 – Proposed Locations for Wi-Fi zones

Fig 52 Kumarswamy_1 Wi-Fi Zones

Kumaraswamy_1 – Proposed Wireless backhaul Link for Root AP # 1

Fig 53 Kumarswamy_1 Wireless Link for AP#1

Kumaraswamy_1 – Proposed Wireless Link for Root AP # 2 from Root AP Location 1

Fig 54 Kumarswamy_1 Wireless Link for AP#2

Kumaraswamy_1 – Proposed Wireless backhaul Link for Root AP # 3 from Root AP # 2

Fig 55 Kumarswamy_1 Wireless Link for AP#3

Kumaraswamy_1 Summary

- Total Wi-Fi zones: 3
- Number of PTP links: 3
- Root AP # 1, # 2 & # 3 to be connected on Wireless Backhaul link on daisy chain
    - Link 1 distance 200 M
    - Link 2 distance 870 M (To be connected from Root AP # 1)
    - Link 3 distance 690 M (To be connected from Root AP # 2)

Kumarswamy_2 – Coverage Area

Fig 56 Kumarswamy_2 Coverage Area

Kumarswamy_2 – Locations for Wi-Fi zones

Fig 57 Kumarswamy_2 Wi-Fi Zones

Kumaraswamy_2 – Wireless Link for Root AP # 1 from Kumaraswamy_1 Root AP # 1

Fig 58 Kumarswamy_2 Wireless Link for AP#1

Line of Sight Details

1. KIOM to C2

2. KIOM to C3

3. KIOM to C4

4. KIOM to IN Gate

Note :
All the LoS locations needs to
reconfirmed in site
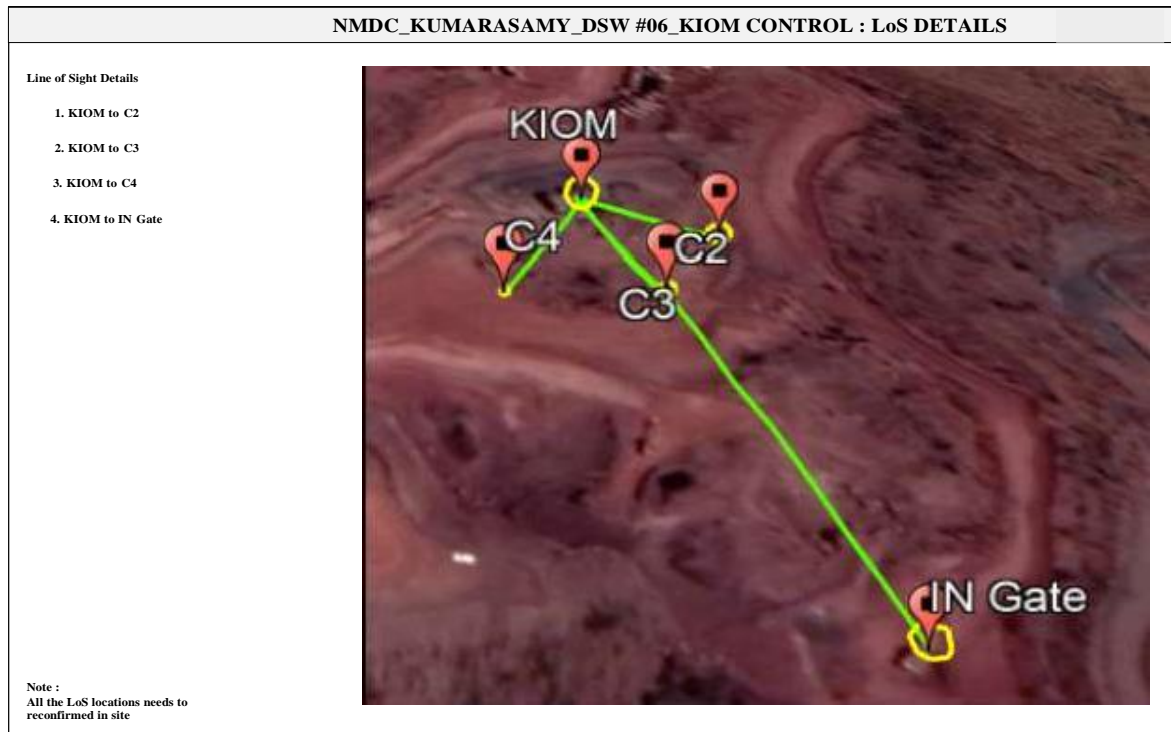
Fig 59 Kumarswamy_2 LoS Details for C Gates

Line of Sight Details

1. KIOM to Out Gate

2. Out Gate to B1

3. Out Gate to B2

Note :
All the LoS locations needs to
reconfirmed in site
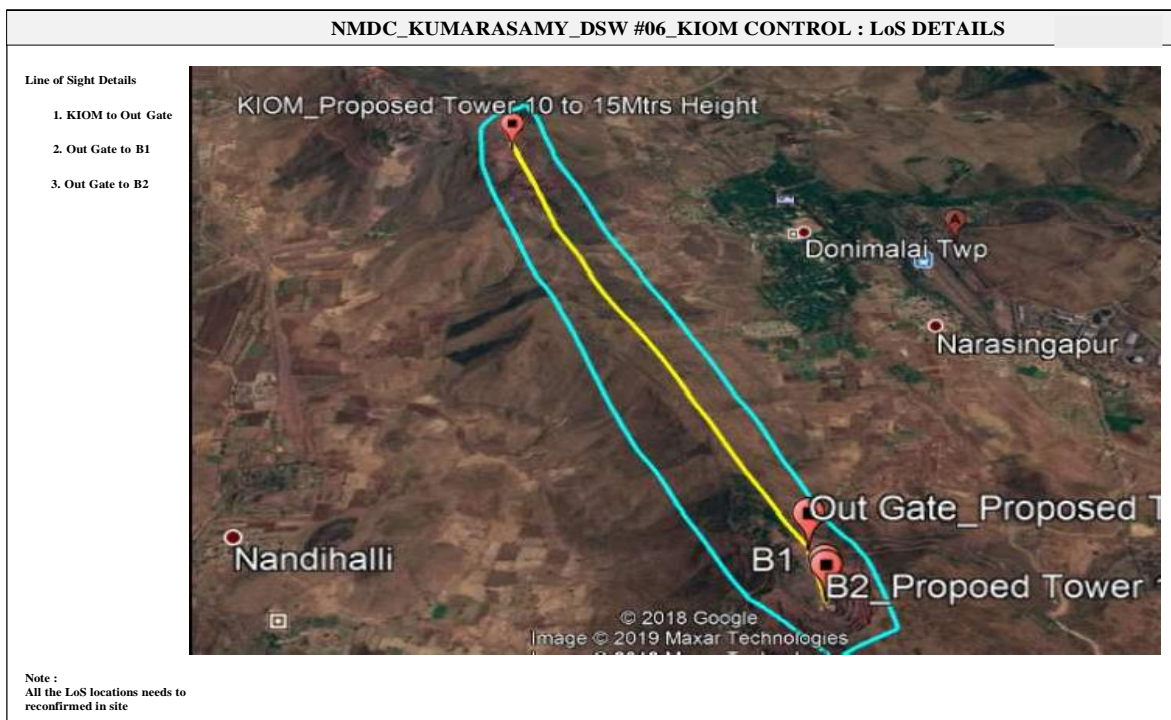
Fig 60 Kumarswamy_2 LoS Details for B Gates

Kumaraswamy_2 Summary

- o Total Wi-Fi zones: 1
- o Number of PTP links: 1
- o To be connected from Kumarswamy_1 Location 1 to Kumarswamy_2 Location 1 on Wireless backhaul link
    - o Link 1 distance 5000 M

Wi-Fi access for end-Points at Weighbridges
- o 4 weighbridge zones
- o P2P links – 4
    - o Max distance: 400m
    - o Fiber backhaul available
- o Wi-Fi zones – 4

Diamond Mine Panna

Network Design Single Line Diagram
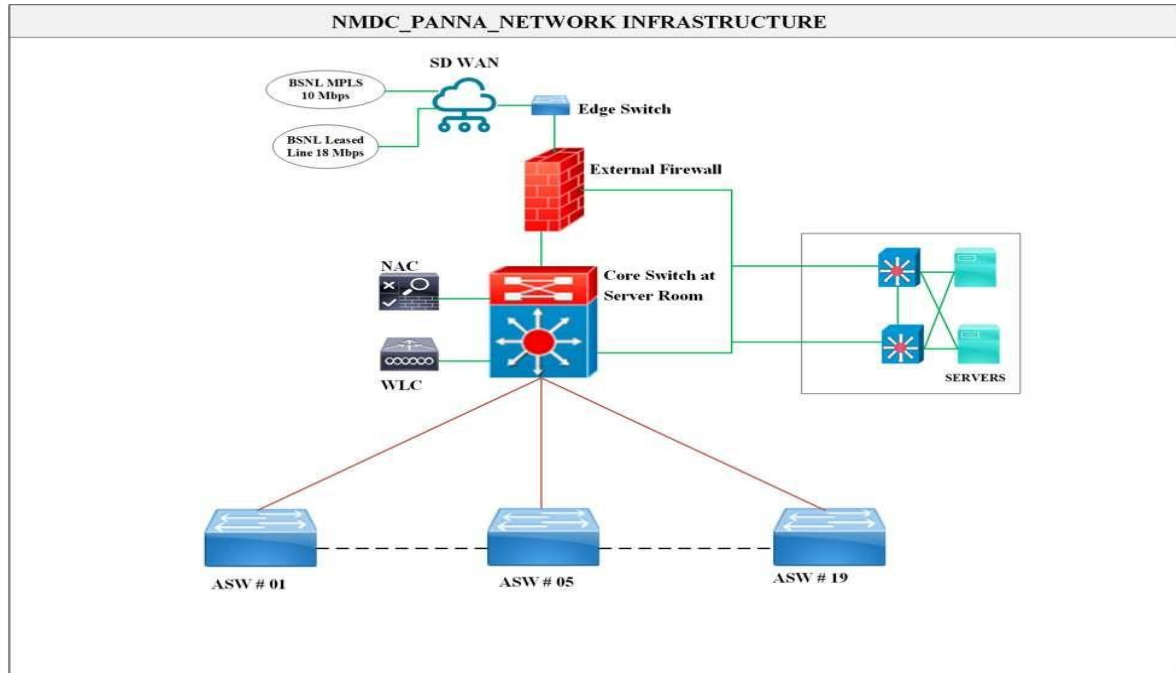
Fig 61 Panna Single Line Diagram
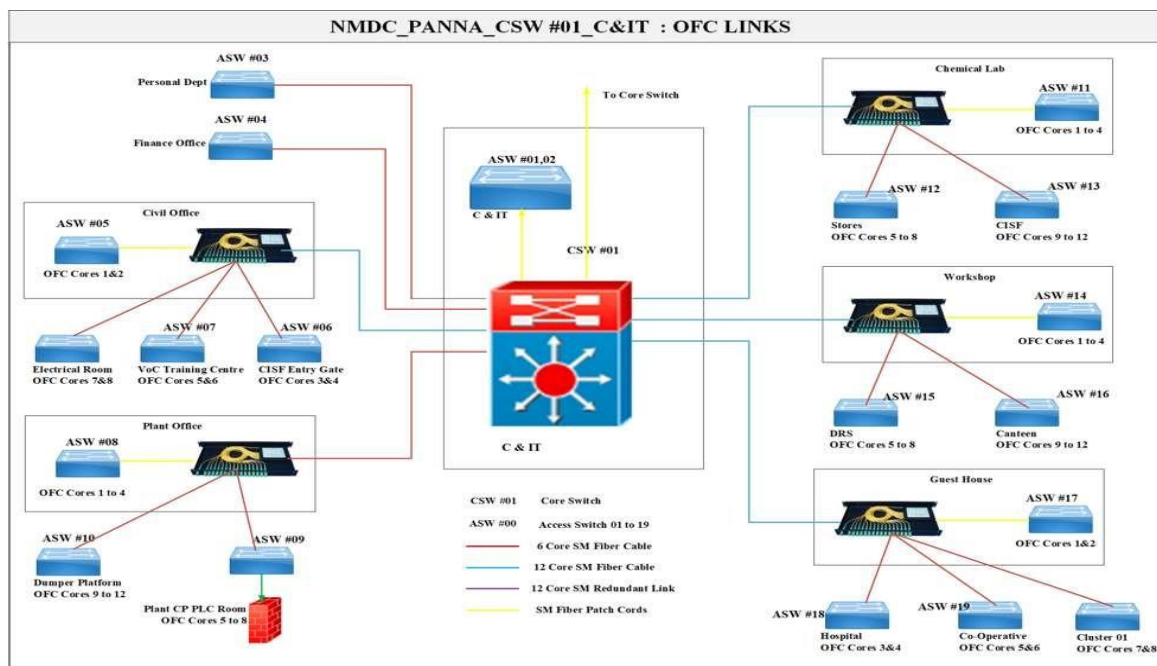
Fig 62 Panna Distribution Switch#1 Network Diagram

Sponge Iron Unit Paloncha

Network Design Single Line Diagram
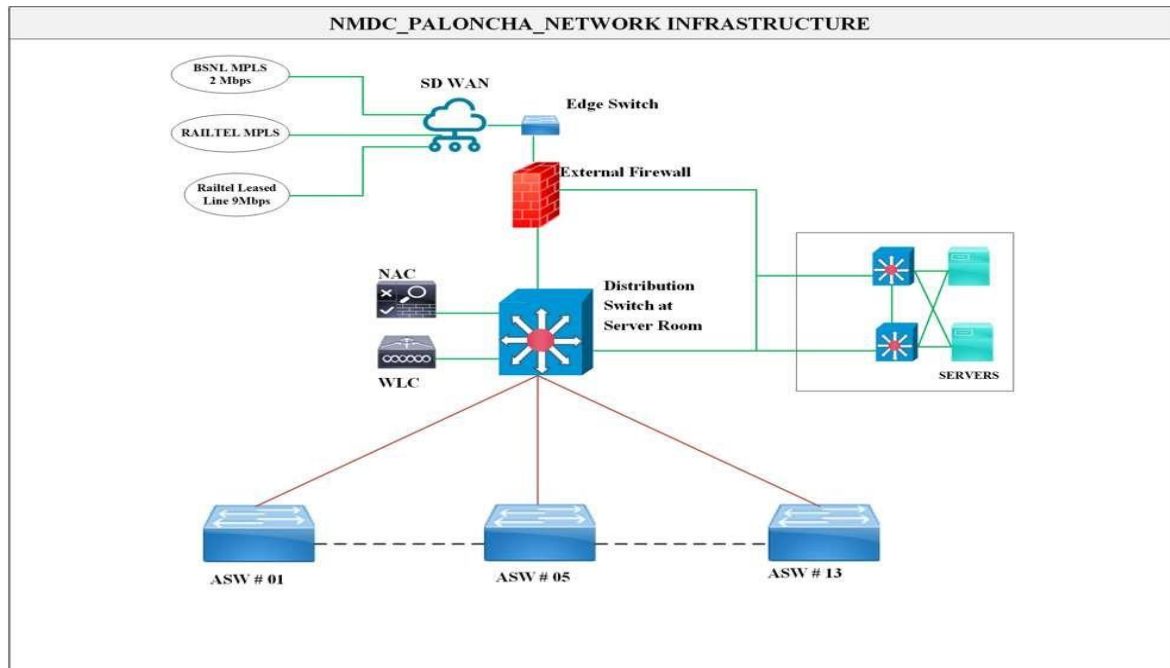
Fig 63 Paloncha Single Line Diagram
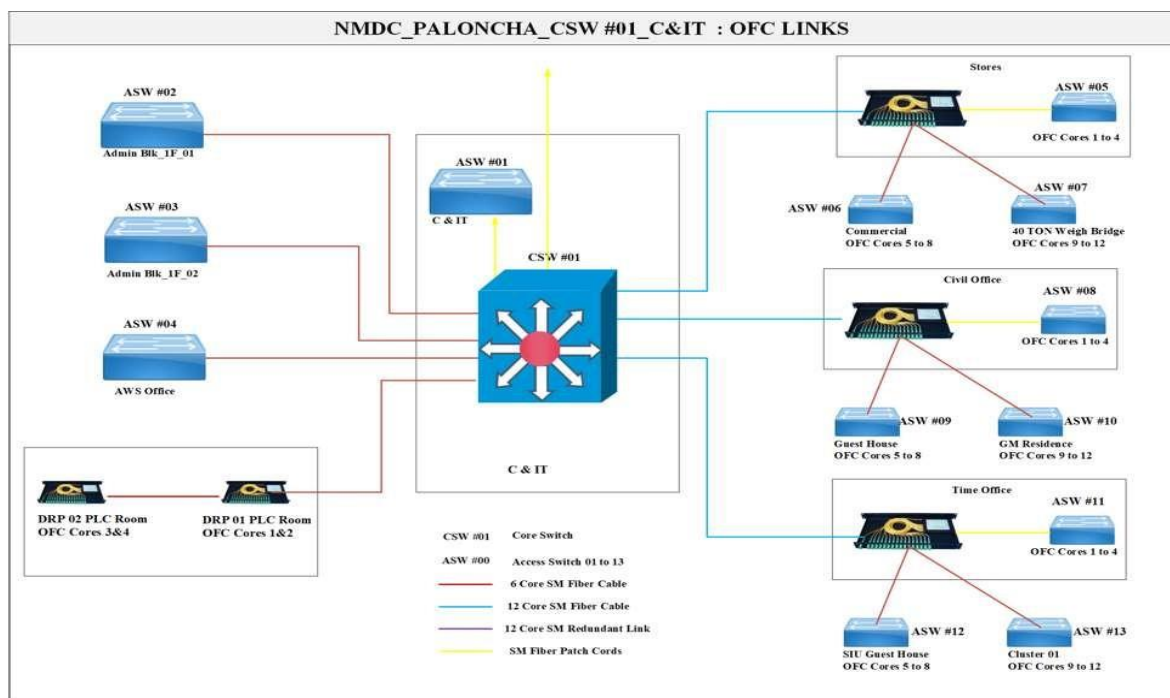
Fig 64 Paloncha Switch#1 Network Diagram

Glossary

Acronym	Expansion
BG	Bank Guarantee
BOQ	Bill of Quantity
BOM	Bill of Material
CSP	Cloud Service Provider
DC	Data Center
DR	Disaster Recovery
EMS	Enterprise Management System
ERP	Enterprise Resource Planning
ILL	Internet Lease Line
IPR	Intellectual Property Rights
IOPS	Input/output operations per second
LAN	Local Area Network
LB	Load Balancer
ITI LTD	Managed Service Provider
MPLS	Multi-Protocol label Switching
NMS	Network Management System
NOC	Network Operation Center
OEM	Original Equipment Manufacturer
QP	Quarterly Payment
RAM	Random Access Memory
RTO	Recovery Time Objective
RPO	Recovery Point Objective
SPOF	Single Point of Failure
SAS	Serial Attached SCSI
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SI	System Integrator
SLA	Service Level Agreement
SSD	Solid State Drive

TC	Total Cost
TP	Total Payment
VLAN	Virtual Local Area Network
VM	Virtual Machines
WAN	Wide Area Network

Annexure – II

Technical Specifications

A. Bill of Quantity

1.1. DC & DR Hardware

Sl. No.	DC Hardware Description	Qty	Technical Specs Page No.
1	SAP HANA Appliance S/4 – 3 TB	2	15, 16-18
2	SAP HANA Appliance SRM – 1.5 TB	2	15, 16-18
3	SAP HANA Appliance BW – 1.5 TB	2	15, 16-18
4	SAP HANA Appliance for Dev – 768 GB	1	16-18
5	SAP HANA Appliance for Quality - 3 TB	1	16-18
6	OS Cluster software	As applicable	17
7	Blade Enclosure (as per OEM solution for 24 blades)	As applicable	18-21
8	Blades for Application Servers - SAP Environment	10	21-28
9	Blades for ADS, Mail, Backup & Misc Servers	4	23-28
10	Blades for EMS Servers in HA 2+2	4	22-28
11	SAN Storage	1	28-31
12	SAN Switches	2	35-38
13	Backup Device with Backup SW for disk backup	1	31-35
14	Tape Library with backup SW	1	33-34
15	Data Centre Core Switches	2	38-39
16	ToR Switch 24 SFP+ for DC	4	39-41
17	1G Copper Switch for SAP HANA Backup – 24 ports	1	44-46
18	1G copper switch for Management – 48 ports	2	41-44
19	Blades for Legacy Servers	6	23-28

Sl. No.	DR Hardware Description	Qty	Technical Specs Page No.
1	SAP HANA Appliance DB – 3 TB	1	15, 16-18
2	SAP HANA Appliance SRM – 1.5 TB	1	15, 16-18
3	SAP HANA Appliance BW – 1.5 TB	1	15, 16-18

4	Blade Enclosure (as per OEM solution for 7 blades)	As applicable	18-21
5	Blades for Application Servers - SAP Environment	5	21-28
6	Blades for ADS, Mail, Backup & Misc Servers	2	23-28
7	SAN Storage	1	28-31
8	SAN Switches	2	35-38
9	Backup Device with Backup SW for disk backup	1	31-35
10	Core Switches	1	38-39
11	ToR Switch for DR - 24 SFP+	2	39-41
12	1G copper switch for Management – 48 ports	1	41-44

Sl. No.	Local Server Hardware	Qty	Technical Specs Page No.
1	xMII Rack Servers	6	46-50
2	ADS, Antivirus & Patch Mgmt Servers (Rack servers)	6	47-50

1.2.   DC & DR Software

Sl. No.	DC Software Description	Make & Model	Qty	Technical Specs Page No.
1	Operating System for App Servers	SUSE Linux for SAP 2Skt Unlimited Guest with HA	10	
2	OS for ADS, Mail, Backup & Misc Servers	WinSvr STD 2019 OLP Core Licenses	4	
3	OS for EMS Servers	WinSvr STD 2019 OLP Core Licenses	4	
4	Virtualization SW	VMWare vCentre Standard with 5 yrs	1	
5		VMWare vSphere Enterprise Plus with 5 yrs	48	
6	OS for HQ & Plant Servers	WinSvr STD 2019 OLP Core Licenses	3	
7	OS for HQ & Plant Servers	SUSE Linux for SAP 2Skt Unlimited Guest OS	3	

8	EMS	Enterprise management software	1	50-56
9	Microsoft Active Directory CAL licenses	Microsoft & Active Directory	1000	

Sl. No.	DR Software Description	Make & Model	Qty	Technical Specs Page No.
1	Operating System for App Servers	SUSE Linux for SAP 2Skt Unlimited Guest OS	5	
2	OS for ADS, Mail, Backup & Misc Servers	WinSvr STD 2019 OLP Core Licenses	2	
3	Virtualisation SW	VMWare vCentre Standard with 5 yrs	1	
4		VMWare vSphere Enterprise Plus with 5 yrs	14	

Sl. No.	Local Server Software	Make & Model	Qty	Technical Specs Page No.
1	Operating System for xMII Servers	SUSE Linux for SAP 2Skt Unlimited Guest OS	6	
2	ADS, Antivirus & Patch Mgmt Servers operating system	Windows server 2019 standard operating system	6	

1.3. Firewall

Sl. No.	Network Components	UoM	Qty	Technical Specs Page No.
WAN Network Interface				
Firewalls: Accepted Makes: Fortinet, Palo Alto, Cisco with 5 Year Support				
1	Firewall – Type 1	Nos.	2	56-58
2	Firewall – Type 2	Nos.	11	58-61
3	Firewall – Type 3	Nos.	6	64-67
4	Firewall – Type 4	Nos.	4	67-70

5	Firewall – Type 5	Nos.	20	70-73
6	Firewall – Web Application Firewall	Nos.	2	61-64
7	Centralized Management, log and analysis license with 5 -year support. up to 100x firewall devices/administrative, supplied along with 5 years 24 x 7 support along with hardware appliance	Nos.	1	
8	Free of charge training to 20-people team of Network Engineers from NMDC to be provided by OEM at a centralized place covering all aspects of operations and maintenance of the Firewalls	Nos.	1	

1.4. Switch, Indoor Wireless, NAC, EMS etc.

SI. No.	Network Components	UoM	Qty	Technical Specs Page No.
Ethernet Switches and Access Points at NMDC Locations				
Accepted Makes: Extreme, HPE, Cisco with 5 Year Support				
1	Core Switch - Type 1	Nos.	6	73-74
2	Core Switch - Type 2	Nos.	1	74-76
3	10G-ER SM SFPs for distribution Switches to core Switches links	Nos.	08	
4	10G-LR SM SFPs for distribution Switches to Access and Distribution Switches	Nos.	64	
5	Distribution Switch – Type 1	Nos.	7	76-77
6	Distribution Switch – Type 2	Nos.	11	77-78
7	1G-LX SM SFPs for distribution Switches to Access Switches links	Nos.	478	
8	10G-LR SM SFPs for distribution Switches to access Switches links	Nos.	200	
9	1000BASE-T RJ45 SFP Transceiver	Nos.	20	
10	Access Switch – Type 1	Nos.	305	78-79

11	Access Switch (Industrial Grade) – Type 2	Nos.	153	79-80
12	Access Point (Indoor)	Nos.	300	81-82
13	Wireless LAN Controller for Access Points, 5 year warranty & NBD support	Nos.	10	82-84
14	NAC licenses for switches and access points, 5 year warranty & NBD support	Nos.	6	84-85
15	OEM EMS for Integrated Monitoring of (Industrial, Access, Distribution and Core) Switches and Wireless Access Points, 5 year NBD support	Nos.	6	86-88
16	VM for installation of NAC and EMS - 4 CPU x86 cores, 64GB RAM, 500GB x 2 disks in failover RAID	Nos.	6	
17	Free of charge training to 20-people team of Network Engineers from NMDC to be provided by OEM at a centralized place covering all aspects of operations and maintenance of the Switches, APs, NAC, WLC, EMS	Nos.	1	

1.5.   WiFi

Sl. No.	Network Components	UoM	Qty	Technical Specs Page No.
Outdoor Wi-Fi Zone - Accepted Make: Cambium, Ruckus, Cisco, Aruba, Radwin				
	At Dumper Platforms, PoL and Workshops			
1	Outdoor (IP66 or better rated) 90~120 sector 802.11ac WLAN AP with Tilt bracket & PoE Injector, 5-year extended warranty to be included. AP with set of 2 antenna (for 240-degree coverage) to be included	Nos.	58	88-90
2	Supply & Installation of Tower / Pole, 5m, Galvanized steel, with grouting base and accessories with Lightning Arrestors	Nos.	29	
	P2P Radio Links (for Workshop @ Bacheli)			

1	5 GHz PTP Radio, Integrated High Gain Antenna (ROW) with power lead, 5-year extended warranty, IP66 or better rated	Nos.	6	
2	Coaxial Cable Grounding Kits for 1/4" and 3/8" Cable	Nos.	12	
3	LPU and Grounding Kit (1 kit per ODU)	Nos.	6	
4	POWER SUPPLY, 30W, 56V - Gbps support	Nos.	6	
5	Tilt Bracket Assembly	Nos.	6	
6	Supply & Installation of Tower / Pole, 15m, Galvanized steel, with grouting base and accessories with Lightning Arrestors	Nos.	3	
Wi-Fi Zones and P2P links for mine coverage (Shovels, Dozers etc.) & weighbridges at KIOM				
	Wi-Fi Zones			
1	Outdoor (IP66 or better rated) 90~120 sector 802.11ac WLAN AP with Tilt bracket & PoE Injector, 5-year extended warranty to be included. AP with set of 2 antenna (for 240-degree coverage) to be included	Nos.	84	88-90
2	Supply & Installation of Tower / Pole, 5m, Galvanized steel, with grouting base and accessories with Lightning Arrestors	Nos.	28	
	P2P Links			
1	Coaxial Cable Grounding Kits for 1/4" and 3/8" Cable	Nos.	92	
2	LPU and Grounding Kit (1 kit per ODU)	Nos.	46	
3	5 GHz PTP Radio, Integrated High Gain Antenna (ROW) with power lead, 5-year extended warranty, IP66 or better rated	Nos.	46	
4	POWER SUPPLY, 30W, 56V - Gbps support	Nos.	46	
5	Tilt Bracket Assembly	Nos.	46	
6	1PPS GPS Sync generator	Nos.	46	
7	PoE Gigabit DC Injector, 15W Output at 30V, Energy Level 6 Supply	Nos.	46	
8	Supply & Installation of Tower / Pole, 15m, Galvanized steel, with grouting base and accessories (some will be mounted on Wi-Fi zone towers)	Nos.	17	

9	Free of charge training to 20-people team of Network Engineers from NMDC to be provided by OEM at a centralized place covering all aspects of operations and maintenance of the Outdoor WAPs	Nos.	1	
Point-to-Multipoint Radio for 5 network zones for Wi-Fi coverage (750m radius) at Weighbridges at KS-2 mines (for budgetary pricing only)				
1	PMP Radio, IP66 or better rated, 240-degrees coverage (may need 2 base stations if each unit provides only 120-degree coverage), with all accessories and 5-year extended warranty.	Nos.	5	
2	Remote radios for the PMP, 4 radios per zone, 240-degree coverage with all accessories and 5-year extended warranty	Nos.	20	
3	Supply & Installation of Tower / Pole, 5m, Galvanized steel, with grouting base and accessories, with Lightning arrestors	Nos.	25	
4	Supply & Installation of 15m Tower (3-legs), with all accessories for outdoor-Wi-fi AP installation, with Lightning arrestors	Nos.	5	

1.6. Campus Backbone Cabling

SI. No.	Network Components	UoM	Qty	Technical Specs Page No.
Campus Backbone Cabling - Accepted Makes: CommScope Netconnect, Belden, Corning, Cmon				
1	12-Core SM double jacketed Outdoor armoured cable	Meters	189,500	91
2	6-Core SM double jacketed Outdoor armoured cable	Meters	80,500	91
3	48-fiber 2U, rack mounted fiber optic patch panels, for terminating OSP cables, with fusion splice trays, fully loaded with Duplex-LC SM adapters and 48 numbers of LC SM pigtails (48 numbers per panel)	Nos.	50	90-92

4	24-fiber 1U rack mounted fiber optic patch panels, for terminating OSP cables, with fusion splice trays, fully loaded with Duplex-LC SM adapters and 24 numbers of LC SM pigtails (24 numbers per panel)	Nos.	234	90-92
5	LC-LC Duplex SM Patch Cords, 3 meter	Nos.	626	91-92
Closed Steel Racks -				
1	42U Racks as per specifications with vertical 2 PDUs, SNMP enabled (for Core Switches)	Nos.	11	99-100
2	42U Racks as per specifications with vertical 2 PDUs, surge protected (for Distribution Switches)	Nos.	21	99-100
3	24U Racks as per Specifications, with horizontal PDUs (IP Rated)	Nos.	153	99-100
4	24U Racks as per Specifications, with horizontal PDUs only (Non-IP Rated)	Nos.	227	99-100
Horizontal Cabling - Accepted Makes: CommScope Netconnect, Belden, Panduit				
1	1U, 24-port Cat6A UTP Unloaded Jack Panel with rear Cable Support bar	Nos.	9	94-95
2	Cat6A UTP Patch Cord (7-feet)	Nos.	462	93-94
3	Cat6A UTP Information Outlet at DC Rack End	Nos.	362	94
4	1-port Face Plate	Nos.	161	98
5	45mm x 45mm Backbox	Nos.	130	
6	IP rated Backbox for Faceplates and Information Outlets	Nos.	50	
7	Cat6A UTP Cable	(305 Mtr.) Roll	20	92-93
8	Plugs for Modular Plug Terminated Links, for Wi-Fi APs and CCTV	Nos.	275	95
9	Cat6A UTP Information Outlet at End-User Rack End	Nos.	100	94
Horizontal Cabling - Accepted Makes: CommScope Netconnect, Belden, Panduit				
1	1U, 24-port Cat6 UTP Unloaded Jack Panel with rear Cable Support bar	Nos.	234	97-98
2	Cat6 UTP Patch Cord (7-feet)	Nos.	5,600	96

3	Cat6 UTP Information Outlet at DC Rack-End	Nos.	2,800	96-97
4	1-port Face Plate	Nos.	1,401	98
5	45mm x 45mm Backbox	Nos.	982	
6	IP rated Backbox for Faceplates and Information Outlets	Nos.	510	
7	1 Port Surface Mount Box	Nos.	1,294	98
8	Cat6 UTP Cable	(305 Mtr.) Roll	472	95-96
9	Cat6 UTP Information Outlet at End-User Rack-End	Nos.	2,800	96-97
UPS - Accepted Makes: APC, Emerson (Vertiv), Delta, Numeric				
1	Supply, Installation, Testing and Commissioning of 1 KVA UPS system (prefer 19' rack mountable unit) for Distribution and access Switches at Bacheli, Kirandul, Donimalai, Panna and Paloncha. 1KVA rating, SNMP manageable. Supply should include 30-minute battery back-up batteries of 65AH, 12V, SMF related electrical protection accessories and rack, 3-year on-site warranty and maintenance	Nos.	259	101-105
2	Supply, Installation, Testing and Commissioning of (N) 30KVA UPS System for Central Distributor to support core switches, Servers, WAN Optimizers, ILL load balancers, and other networking equipment along with 30-minutes battery back-up (about 40 batteries of 65AH, 12V, Lead Acid, SMF) along with Battery rack, MCB protection gear and all other accessories - Bacheli, Kirandul, Donimalai, Panna and Paloncha. UPS to be SNMP manageable. 30kVA rating. Supply should include 3-year on-site warranty and maintenance	Nos.	5	105-109
3	Supply & Installation of Grounding Pit and services- for servers and communication	Nos.	14	101
4	Supply & Installation of Lightning arrestors and grounding pit	Nos.	14	101

1.7. OFC Laying

Sl. No.	Network Components	UoM	Qty	Technical Specs Page No.
1	Installation (Trenching, cable pulling through HDPE pipes, Manholes every 2KMs or 2 right angle bends) Testing and Commissioning of Optical Fibre Links along with supply of ISI marked / TEC approved HDPE pipe	Meters	270,000	
2	Splicing & testing of OFC (Pigtails)	Nos.	284	
3	Installation of Racks, Earthing etc.	Nos.	412	
4	Installation, Testing, Commissioning and Certification of Horizontal Cable Links along with requisite Capping & Casing /PVC Conduits /HDPE Pipes	Nos.	3,162	

1.9. One Time Charges for Co-location and Managed Services

Sl. No.	Description	UoM	Qty	Technical Specs Page No.
1	Supply of 42 U, 800 mm x 1200 mm Server Rack. (DC-4, DR-2) Supply of 42U, 800 mm x 1000 mm Server Rack (DC-6, DR-2)	Nos.	14	
2	**Powered On** Colocation Full Rack space. (6) KVA Rated with Bundled Power. (DC)	Nos.	10	
3	SS Cage with Biometric Access, CCTV Camera.	Lot	1	
4	**Powered On** Colocation Full Rack space. (6) KVA Rated with Bundled Power. (DR)	Nos.	4	
5	Copper Cross Connect Charges. Cat 6	Nos.	8	
6	Seating Space in DC for OEM/ IP/ SI/ NMDC	Nos.	1	
7	**Colocation Managed Services**	Lumpsum	1	

1.10. Colocation Services

Sl. No.	Description	UoM	Qty	Technical Specs Page No.
1	Supply of 42 U, 800 mm x 1200 mm Server Rack. (DC-4, DR-2) Supply of 42U, 800 mm x 1000 mm Server Rack (DC-6, DR-2)	Nos.	14	
2	**Powered On** Colocation Full Rack space. (6) KVA Rated with Bundled Power. (DC)	Nos.	10	
3	SS Cage with Biometric Access, CCTV Camera.	Lot	1	
4	**Powered On** Colocation Full Rack space. (6) KVA Rated with Bundled Power. (DR)	Nos.	4	
5	Copper Cross Connect Charges. Cat 6	Nos.	8	
6	Seating Space in DC for OEM/ IP/ SI/ NMDC	Nos.	1	

1.11. Managed Services

Sl. No.	Description	UoM	Qty	Technical Specs Page No.
1	Colocation Managed Services	Lumpsum	1	112-119

1.12. NOC

Sl. No.	Network Components	Qty	UoM	Technical Specs Page No.
1	Desktop for NOC	4	Nos.	119
2	Console/Screen (LFD) for NOC room	2	Nos.	119

Note: Seating arrangement to be provisioned by NMDC for 6 persons

B. Technical Specification

2.1. DC & DR Hardware

i) Hana Servers for DC & DR

a) SAP S/4 HANA Prd Box

Sl. No.	Item	Description
1	**Make & Model**	**Accepted Make: HPE/ DELL/ CISCO**
2	SAP HANA S/4 Prd Server	• SAP HANA Certified Appliance for >= 3TB • Make & Model proposed should be available in the SAP HANA website. • Document to be submitted along with the technical BOQ • HANA Appliance should be fully factory configured
3	System	• SAP certified Single Node Scale-up HANA Box with latest Cascade lake CPU based server.
4	Processor	• 4 X Intel 8276 Platinum Processor, 28 Core, 2.2 Ghz
5	Memory	• 3 TB DDR4 RAM or more
6	Networking	• Minimum 8 X 10 Gbe Ethernet ports with SFP+ Modules for data and replication

b) SAP BW/4, SRM HANA Prd Boxes

Sl. No.	Item	Description
1	**Make & Model**	**Accepted Make: HPE/ DELL/ CISCO**
2	SAP HANA BW & SRM Prd Server	• SAP HANA Certified Appliance for >= 1.5TB • Make & Model proposed should be available in the SAP HANA website. • Document to be submitted along with the technical BOQ • HANA Appliance should be fully factory configured
3	System	• SAP certified Single Node Scale-up HANA Box with latest Cascade lake CPU based server.
4	Processor	• 2 X Intel 8276 Platinum Processor, 28 Core, 2.2 Ghz
5	Memory	• 1.5 TB DDR4 RAM or more
6	Networking	• Minimum 4 X 10 Gbe Ethernet ports with SFP+ Modules

		for data and replication

c) *SAP HANA Quality Box*

Sl. No.	Item	Description
1	**Make & Model**	**Accepted Make: HPE/ DELL/ CISCO**
2	SAP HANA Quality Server in DC	• SAP HANA Certified Appliance for >= 3TB • Make & Model proposed should be available in the SAP HANA website. • Document to be submitted along with the technical BOQ • HANA Appliance should be fully factory configured
3	System	• SAP certified Single Node Scale-up HANA Box with latest Cascade lake CPU based server.
4	Processor	• 4 X Intel 8276 Platinum Processor, 28 Core, 2.2 Ghz
5	Memory	• 3 TB DDR4 RAM or more
6	Networking	• Minimum 8 X 10 Gbe Ethernet ports with SFP+ Modules for data and replication

d) *SAP HANA Dev Box*

Sl. No.	Item	Description
1	**Make & Model**	**Accepted Make: HPE/ DELL/ CISCO**
2	SAP HANA Dev Server in DC	• SAP HANA Certified Appliance for >= 768 GB • Make & Model proposed should be available in the SAP HANA website. • Document to be submitted along with the technical BOQ • HANA Appliance should be fully factory configured
3	System	• SAP certified Single Node Scale-up HANA Box with latest Cascade lake CPU based server.
4	Processor	• 2 X Intel 8276 Platinum Processor, 28 Core, 2.2 Ghz
5	Memory	• 768 GB DDR4 RAM or more
6	Networking	• Minimum 4 X 10 Gbe Ethernet ports with SFP+ Modules for data and replication

e) Other General Specification

Sl. No.	Item	Description
1	Disk for Persistence Storage	• At least 4 times the RAM capacity in RAID5 with persistence storage with SSD's.
2	Operating System	• Latest version of "Suse Linux Enterprise Edition for SAP" • OS version certified for the SAP HANA should be proposed for all the CPU's populated • Supplied Operating System should be with Priority subscription for 5 years

3	High Availability Solution	• Clustering solution to be provided for application and HANA Boxes
		
		• The HA solution between the two HANA boxes should be integrated with cluster software and HANA System Replication.
		
		• The HA solution should provide the automated failover functionality within the nodes in case of:
		
		  • Hardware failure in the box
		  • OS failure
		  • Network / Link failure
		  • Database Server failure
		  • Failover of Active Database instance from Primary node to Secondary Node and vice-versa
		  • The Cluster software should support Disk based or Node Based Quorum implementation to prevent "split-brain" scenarios in Cluster Setup

4	Cluster Network	The heartbeat network, required to setup the HA solution, should be separate from the actual Data and User network. Minimum 2 nos. 24 port 1G Ethernet switches should be included in the solution to setup the cluster and management network between 2 HANA boxes.
5	System monitoring & Management	Proposed Infrastructure should have dedicated remote management functionality; management of Infrastructure should include following, • Must have the capability to provide proactive notification of actual or impending component failure alerts. • Automatic event handling should be supported to configure actions to notify appropriate users of failures through e-mail/SMS etc. • Automatic event alert forwarding to OEM remote support

		center and proactively call-logging system.
6	Power Supply & Fan	Power supplies and Fans should be redundant and hot-swappable
7	Warranty & Support Services	5 Years 24 x 7 Support with 6hr Call to resolution. Warranty shall be directly from OEM including Software upgrades/updates. The OEM should have the capability to offer lifecycle services like OS Upgrades, Patch Management and HANA DB Upgrade.
8	Bill of Materials	The vendor shall give make, model, part nos. of every component which will be cross verified by OEM.
9	Manufacturer Authorization Letter	Manufacturers Authorization Letter Specific to this tender must be submitted. Tender submitted without MAL will be rejected.

ii) Application Servers for DC & DR

a) Blade Enclosure

Sl. No.	Item	Description
1	**Make & Model**	**Accepted Make: HPE/ DELL/ CISCO**
	Solution Requirement	- Proposed solution should support provisioning virtual, physical and container infrastructure from pools of compute, storage and networking resources - Solution should have single console provisioning for compute, storage and server-side network configuration and direct attach storage (DAS). Direct connect midplane should deliver 14 Tbps of bandwidth. FC SAN should be available - Solution should support software defined templates to quickly make changes to the infrastructure. Template should include server BIOS, firmware, boot order, RAID, storage configuration and network config of the infrastructure required for workload - Solution should support scripting to reassign compute resources to different workloads to effectively utilize the infrastructure (re provision compute resources from one workload to another)
	Blade Chassis	- Solution to house the required number of blade servers in smallest number of enclosures. - Should support two socket and four socket blades in the same enclosure, occupying a max of 7U/10U rack height

		• Should support minimum 8 number of 2 CPU Servers or 4 number of 4CPU servers Or Higher.
		• Blade Chassis backplane engineered with 14Tbps or higher Chassis backplane bandwidth.
		• Should support six interconnect bays to configure 3+3 redundancy
		• Should support built-in management software appliance in redundancy with separate management network from production network
		• Should support technology built-in to every chassis for Auto-Discovery of resources
		• Chassis should provide display port and USB port to connect Laptop/Monitor locally
		• Should support linking multiple enclosures (at least 20 enclosures) together to form single management ring to reduce complexity and provide single console of management for connected enclosures
	Interconnects support	• Should support housing of FCoE, Ethernet, FC and SAS interconnect fabrics offering redundancy as a feature. Also should support network switch with 25/50Gb downlinks and 100G uplink to DC switch
	Converged interconnect	• Redundant Interconnect modules shall be integrated within the chassis such that uplinks from the chassis can be directly connected to core LAN/SAN switches
		• Interconnect should support 25Gbps downlinks to the Blades in redundancy supporting carving of each port into at least four ports.
		• Should support at least six QSFP+/QSFP28 for external uplink to choose Ethernet and FC uplinks as needed
		• Should support aggregation of multiple enclosures to consolidate data center network connections, reduce hardware and to scale network bandwidth across multiple enclosures.
		• At-least 60 /36 servers should be supported per aggregation. Layer 2 network traffic should be switched within enclosure aggregation (without using top of the rack switch) and provide when multiple chassis aggregated, switching latency between enclosures should not exceed 1.0 micro-second for Ethernet
	Blade Chassis Interconnect	• Redundant Ethernet Switches should have at least 25Gb downlinks to each blade server should support 40G and 100G uplink to DC switch. and at least 8x 10GbE SFP+

		uplink ports and Redundant Blade SAN Switches each with 4x 16 Gbps FC SFPs uplinks
		Or
		• Redundant interconnects and each interconnect should have at least 25Gb downlinks to each blade server and at least 8x 10GbE SFP+ uplink ports and at least 4x 16 Gbps FC SFP's uplinks ports and should support 40G and 100G uplink to DC switch.
	Power Supply	• The enclosure should be populated fully with power supplies of the highest capacity available with the vendor. Power supplies should support N+N as well as N+1 redundancy configuration, where N is greater than 1. • Should offer a single-phase power subsystem enabled with technologies for lower power consumption and offering Platinum energy efficiency. Vendors should provide documents certifying the claims.
	Cooling	• Redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics
	System Software	Management/controlling software's have to be from the OEM.
	Chassis management capabilities	Solution should support redundant physical management appliances within an enclosure or on multiple connected enclosures with failover and high availability Should support auto-discovery of Compute, Memory, Storage and Fabrics within an enclosure or on multiple connected enclosures. Should support activity, Health and Power LEDs for immediate status Should support software-defined intelligence for configuring profiles to provision compute, storage, fabrics and images Should support Firmware and OS Driver updates for the servers using profile templates to monitor, flag, and remediate Should offer collaborative user interface which support logical resources to physical resources mapping, Smart/advanced Search, Activity Log, HTML5 mobile access, and Customizable Dashboard. Should provide a dedicated 10GbE or higher management network for multi-enclosure communications, separate from data plane

		Should support frictionless Firmware and OS Driver updates using profile templates to monitor, flag, and remediate
		Should support reporting capabilities for 1) asset and inventory information for the devices in the enclosures
		2) thermal and power information, including real-time actual power usage per server and per enclosure
		Reports should be exportable to csv or Microsoft Excel format
	Warranty	5 Years 24x7 onsite support with commitment to resolve the problem within 6 Hours. Support has to be provided directly by OEM during the warranty period.
	Bill of Materials	The vendor has to give make, model, part nos. of every component which will be cross verified by OEM.
	Manufacturer Authorization Letter	Manufacturers Authorization Letter Specific to this tender must be submitted. Tender submitted without MAF will be rejected.

b) Server Blade

Sl. No.	Item	Description
1	**Make & Model**	**Accepted Make: HPE/ DELL/ CISCO**
2	Server	• Offered Blade for SAP Application should be SAP certified. Make & Model offered should be available in the SAP website.
3	CPU	• 2 X Intel Xeon Gold 6252 (2.1GHz, 24-core)
5	Memory	• 768 GB DDR4 RAM or more
6	Disk for server Storage	• Minimum 2 X 600 GB 15K rpm SAS drives
7	Networking	• 1 no of Dual port 25G Adapter/ 1 Nos of Quad port of 10G Adapter and 1* Dual 16Gbps / Dual Port 25GbE or higher Converged Network Adaptor which supports partitioning into Ethernet and FC/iSCSI HBA ports per adaptor port
8	Operating System and Virtualization	• Latest version of "Suse Linux Enterprise Edition for SAP" • Latest Windows Server Enterprise/Datacenter Edition **Virtualization tools** • VMWARE • Supplied Operating System and Virtualization should be

		with subscription for 5 years
		• (Refer Sizing sheet for number of Suse and Windows and VMWare Licenses)
9	High Availability Solution	• Clustering solution to be provided for applications at operating system level.
11	System monitoring & Management	Proposed Infrastructure should have dedicated remote management functionality; management of Infrastructure should include following,
		• Must have the capability to provide proactive notification of actual or impending component failure alerts.
		• Automatic event handling should be supported to configure actions to notify appropriate users of failures through e-mail/SMS etc.
		• Automatic event alert forwarding to OEM remote support centre and proactively call-logging system.
12	Power Supply & Fan	• Power supplies and Fans should be redundant and hot-swappable
13	Warranty & Support Services	• 5 Years 24 x 7 Support with 6hr Call to resolution. Warranty shall be directly from OEM including Software upgrades/updates. The OEM should have the capability to offer lifecycle services like OS Upgrades, Patch Management.
14	Bill of Materials	• The vendor shall give part nos. of every component which will be cross verified by OEM.
15	Manufacturer Authorization Letter	• Manufacturers Authorization Letter Specific to this tender must be submitted. Tender submitted without MAL will be rejected.

iii)   Non-SAP Servers

a) *Enterprise Management Solution Blade Servers (DC & DR)*

SI. No.	Item	Description
1	**Make & Model**	**Specify**
2	CPU	2 x Intel Xeon-Gold 6242 (2.8GHz, 16-core) Processor
3	Memory	24DIMM slots. 256GB Dual Rank Memory DIMMS and support up to 3.0 TB using DDR4 Load Reduced DIMM (LRDIMM).

4	Hard disk drive with carrier	2 x 900 GB 10K RPM hot plug SFF drives

b) ADS, Mail & Misc Blade Servers (DC & DR)

Sl. No.	Item	Description
1	**Make & Model**	**Specify**
2	CPU	2x Intel Xeon-Gold 6242 (2.8GHz/16-core/150W) Processor
3	Memory	24DIMM slots. 384 GB (12 x 32GB DIMMS) Dual Rank Memory DIMMS and support up to 3.0 TB using DDR4 Load Reduced DIMM (LRDIMM).
4	Hard disk drive with carrier	2 x 600GB 15K RPM hot plug SFF drives.

c) Blades for Legacy Servers in DC

Sl. No.	Item	Description
1	**Make & Model**	**Specify**
2	CPU	2 x Intel Xeon-Gold 6238 (2.1GHz, 22-core) Processor
3	Memory	24DIMM slots. 128GB (8*16GB) Dual Rank Memory DIMMS and support up to 3.0 TB using DDR4 Load Reduced DIMM (LRDIMM).
4	Hard disk drive with carrier	2 x 600GB SSD RAID5

d) Other General Specifications

Sl. No.	Item	Description
1	Memory Protection	ECC with multi-bit error protection, Online spare or mirrored memory
2	Storage Controller	It should support Integrated or add-on PCIe 3.0 based 12G SAS Raid Controller with RAID 0, 1 with 1GB of Flash backed write cache onboard
3	Networking features	1 no of Dual port 25G Adapter/ 1 Nos of Quad port of 10G Adapter and 1* Dual 16Gbps / Dual Port 25GbE or higher

		Converged Network Adaptor which supports partitioning into Ethernet and FC/iSCSI HBA ports per adaptor port
4	Interfaces	Minimum of 1* internal USB 3.0 port ,1* internal SDHC card slot and 1* external USB 3.0 port
5	Bus Slots	Minimum of 2 Nos of x16 or higher PCIe 3.0 based slots supporting Converged Ethernet, Ethernet, FC adapters and SAS adaptors
6	Industry Standard Compliance	TPM 2.0 Support Advanced Encryption Standard (AES) or Equivalent or better Triple Data Encryption Standard (3DES) or Equivalent or better SNMP v3 SSL 2.0 DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) Active Directory v1.0 PCIe 3.0 Compliant UEFI (Unified Extensible Firmware Interface Forum) Redfish API
7	Embedded system management	Should support integration with management software to deliver 'composable infrastructure' with a view of resources. This should be flexible and scalable solution providing IT managers with the architecture to implement their software-defined data center (SDDC) and to address the changing business needs and the challenges of today's enterprise data centers Should support Gigabit out of band management port to monitor the servers for ongoing management, service alerting and reporting Should support UEFI to configure and boot the servers securely System should support RESTful API integration System management should support provisioning servers by discovering and deploying 1 to few servers with embedded Provisioning tool System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support

8	System Security	Power-on password
		Administrator's password
		Keyboard password (Quick Lock)
		Remote management On System Management Chipset with SSL encryption, Secure Shell version 2, Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) or equivalent or better on browser, CLP and XML scripting interface, AES and RC4 encryption of video
		External USB port enable/disable
		Network server mode
		Serial interface control
		TPM (Trusted Platform Module) 1.2 or 2.0 option
		Advanced Encryption Standard (AES) or Equivalent or better
		Intel® Advanced Encryption Standard-New Instructions (AES-NI)
9	OS Support	Microsoft Windows Server
		Red Hat Enterprise Linux for SAP (RHEL)
		SUSE Linux Enterprise Server for SAP (SLES)
		VMware
10	System Performance Tuning	1. System should support feature for improved workload throughput for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode without the frequency fluctuations associated with running in turbo mode
		2. System should support workload Profiles for simple performance optimization
11	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.
12	Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable
		2. Should maintain repository for firmware and drivers' recipes to aid rollback or patching of compromised firmware. Should

		also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware
13	Embedded Remote Management and firmware security	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor/Two factor authentication
		2. Server should have dedicated remote management port
		3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware
		4. Server should support agentless management using the out-of-band remote management port
		5. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur
		6. Applications to access the server remotely using popular handheld devices based on Android or Apple IOS should be available
		7. Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128-bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES,3DES or equivalent/better on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console.
		8. Should support RESTful API integration
		9. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support.
		10. Pre-Failure Notification for all active and important components like processors, Memory, Hard drives, etc. and automatic calls logging
14		Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data

	Server Management	center. It should provide an at-a-glance visual health summary of the resource's user is authorized to view.
		The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Appliance alerts
		The Systems Management software should provide Role-based access control
		Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM
		Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.
		Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contracts and status. The Portal should also provide a Personalized dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).
		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.
		The Server Management Software should be of the same brand as of the server supplier.
15	Cloud Enabled Monitoring and Analytics or equivalent through Web Console	1. Offered servers shall have cloud enabled monitoring and for proactive management. All required licenses for same shall be included in the offer. 2. Cloud Enabled Monitoring and shall have capability to provide following: a. Providing Firmware upgrade and patch upgrade recommendations proactively. b. Providing power and support entitlement status. c. Recommendations to eliminate performance bottlenecks and critical events, having capability of proactive recommendation for arresting the issues / problems.

16	Warranty	5 Years 24x7 onsite support with commitment to resolve the problem within 6 Hours. Support has to be provided directly by OEM during the warranty period.
17	Bill of Materials	The vendor has to give make, model, part nos. of every component which will be cross verified by OEM.
18	Manufacturer Authorization Letter	Manufacturers Authorization Letter Specific to this tender must be submitted. Tender submitted without MAF will be rejected.

iv)   Storage for DC & DR

Sl. No.	Item	Description
1	**Make & Model**	**Accepted Make: DELL/ HPE/ CISCO**
2	Converge/ Unified Storage	• Offered Storage array shall be a true converge/ unified storage with a single Microcode/ operating system instead of running different Microcode/ Operating system/ Controllers for File, block and object services respectively. • Offered Storage shall be a flagship Flash array from the OEM, should support only SSD's and shall be clearly published on their website. • The Server & Storage supplied should be from same OEM.
3	Operating System & Clustering Support	• The storage array should support industry-leading Operating System platforms including: Windows 2012, Windows 2016, VMware, Solaris, HPE-UX, IBM-AIX and Linux.
4	Capacity & Scalability	• Refer Sizing sheet for Capacity required for DC & DR • DC Storage capacity should be offered with 85 TB usable capacity using RAID5 with each drive capacity not exceeding 4 TB SSD. • DR Storage capacity should be offered with 48 TB usable capacity using RAID5 with each drive capacity not exceeding 4 TB SSD. • All drives shall be offered with 5 years comprehensive warranty. • Offered Storage array shall support minimum of 480 SSD's • Offered Storage array shall support at-least 500TB Usable capacity for file operations.

5	Cache	• Offered Storage Array shall be given with Minimum of more than 128GB cache in a single unit and shall be scalable to more than 256GB.
		• Cache shall be completely dynamic for read and write operations and vendor shall not offer any additional card / module for write cache operations.
		• Cache shall be used only for Data and Control information. OS overhead shall not be done inside cache.
6	Data Reduction	• Offered Storage shall be Inline de-duplication and compression enabled. Given volume inside the storage array shall support both de-duplication and compression simultaneously.
7	Architecture & Processing Power	• Controllers shall be true active-active so that a single logical unit can be shared across all offered controllers in symmetrical fashion, while supporting all the major functionalities like Thin Provisioning, Snapshot, Cloning, replication etc.
8	No Single point of Failure	• Offered Storage Array shall be configured in a No Single Point of configuration including Array Controller card, Cache memory, FAN, Power supply etc.
9	Disk Drive Support	• Offered storage shall support various SSD capacities drives starting from 400GB onwards.
10	Raid Support, Virtualization & No. of Volumes	• Offered Storage Subsystem shall support Raid level 1, 5, 6 and 10.
		• Offered storage array shall support at-least 4000 Volumes per controller.
11	Data Protection	• In-case of Power failure, Storage array shall have de-stage feature to avoid any data loss.
12	Protocols	• Offered Storage array shall support all well-known protocols like but not limited to FC, ISCSI, SMB 3.0, NFS V4, FTP/SFTP etc.
13	Host Ports and Back-end Ports	• Offered Storage shall have minimum of 12 X 16Gb FC Ports for host connectivity. All types of ports shall be 100% scalable.
		• Offered storage shall have two additional ports for the storage-based replication.
		• Offered storage shall have minimum of 16 SAS lanes running at 12Gbps speed and shall be scalable to 32 SAS lanes without any controller change.
14	Global Hot Spare	• Offered Storage Array shall support distributed Global hot Spare for offered Disk drives.

		• Global hot spare shall be configured as per industry practice.
15	Performance and Quality of Service	• Shall have capability to use more than 30 drives per array group or raid group for better performance. • Offered storage array shall support quality of service for critical applications so that appropriate and required response time can be defined for application logical units at storage. It shall be possible to define different service / response time for different application logical units. • Quality of service engine shall allow to define minimum and maximum cap for required IOPS / bandwidth for a given logical units of application running at storage array. • It shall be possible to change the quality of service Response time ((In both milliseconds as well as Sub-milliseconds), IOPS, bandwidth specification on basis of real time.
16	Thin Provisioning and Space Reclaim	• Offered storage array shall support thin provisioning and Thin Re-claim to make the volume thin for an extended period of time for complete array supported raw capacity. • Offered storage array shall be tightly integrated with VMware so that Eager zero disks layout can be used with thin provisioning and thin re-claim.
17	Maintenance	• Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives.
18	Snapshot/ Point in time copy/ Clone	• The storage array should have support for both controller-based as well as file system-based snapshots functionality (At-least 4000 copies per array).
19	Storage Array Configuration & Management Software	• Vendor shall provide Storage Array configuration and Management software. • Software shall be able to manage more than one array of same family.
20	Remote Replication	• The storage array should support hardware-based data replication at the array controller level across all models of the offered family and license should be included for the entire storage from day one. • The Storage array shall also support three ways (3 Data Centers) replication to ensure zero RPO at any site Near DR and DR in native fashion without using any additional replication appliance.

		• Replication shall support incremental replication after resumption from Link Failure or failback situations.
21	Licenses	• Storage subsystem shall be supplied with Thin provisioning, Snapshot, Clone, Performance Monitoring, Online Raid Migration, Online Volume conversion (thin to thin compressed, thin to thin de-dup etc.), Quality of services, and File services on day 1 for the maximum supported capacity of array.
22	Warranty	• 5 Years 24x7 onsite support with commitment to resolve the problem within 6 Hours. Support has to be provided directly by OEM during the warranty period.
23	Bill of Materials	• The vendor has to give make, model, part nos. of every component which will be cross verified by OEM.
24	Manufacturer Authorization Letter	• Manufacturers Authorization Letter Specific to this tender must be submitted. • Tender submitted without MAF will be rejected.

v)   Backup Solution for DC & DR

a) *Disk Backup for DC & DR*

Sl. No.	Item	Description
1	**Make & Model**	**Shall be provided by OEM who is providing the Hardware**
2	Disk Backup	• Solution /Appliance Should offer Disk to Disk to Tape solution (D-D-T) • Backup device shall be Modular design to allow configuration, add capacity increase performance. • Offered appliance shall be certified to work with at-least 3 Backup application vendor ISV like HPE, Veritas, Dell-EMC, Veeam, Commvault etc. • DC Device should be offered with 60 TB usable and scalable to 120 TB usable space by using not more than 4TB/8TB drives. • DR Device should be offered 30 TB usable and scalable to 60 TB usable space by using not more than 4TB/8TB drives. • Offered device shall also be scalable in native mode (Without de-duplication and compression) • Vendor shall not use any additional staging device in-

			between while moving the data from Disk based backup device to public cloud or object storage
			• Offered device shall have separate dedicated drives for Operating System of appliance and shall not participate in data backup
			• Device shall be offered with dual Hardware Raid Controller card. Each card shall have dual 12Gbps SAS ports
			• Offered device shall support emulation of both VTL and NAS target like CIFS.
			• Offered device shall have capability to deliver selective restore from disk Library itself.
			• Offered device shall have integrated de-duplication license, low bandwidth replication license so that only unique non duplicated block transfers to remote / DR location
			• Offered device shall have intelligence to understand both source-based and target-based de-duplication and shall be integrated with all well-known backup ISVs like Veritas, Commvault and Veeam etc. At-least 3 ISVs shall be supported
			• Offered device shall support receiving non-duplicated data from remote locations or branch office directly from the application servers / Client servers in low bandwidth mode without using any backup or replication-based device at remote location / Branch office
			• Offered device shall have Minimum of 2 x 10/25 Gbps IP, 2 x 16Gbps FC and minimum of 4 x 1Gbps IP connection. License and Transceivers for all ports shall be offered and configured
			• Offered Appliance Fiber channel ports shall support connectivity of servers either directly or via SAN switches while supporting the both source and Target based de-duplication
			• Offered disk-based backup device shall also support encryption functionality
			• When fully populated, offered device shall support rated write performance of more than 16TB per hour in native mode
			• When fully populated, offered device shall supported rated write performance, when enabled with source level de-duplication, of more than 30TB/hr
			• 5 Years 24x7 onsite support with commitment to resolve

		the problem within 6 Hours. Support shall be provided directly by OEM during the warranty period.
		• The vendor shall give part nos. of every component which will be cross verified by OEM.
3		Manufacturers Authorization Letter Specific to this tender must be submitted. Tender submitted without MAF will be rejected.

b) *Tape Library*

Sl. No.	Item	Description
1	**Tape Library**	**Only at DC** **Make & Model:** Should be provided by HW OEM
2	Capacity	• Offered Tape Library shall support Native data capacity of 3.3PB (uncompressed) using LTO-8 Technology. • Shall be offered with Minimum of Four LTO-8 FC tape drive. Drive shall support encryption, minimum 80 media slots from day 1. • Shall be offered with 80 RW LTO-8 Cartridges and 4 Cleaning cartridges • Shall be scalable 270 cartridge slots with additional enclosures
3	Tape Drive Architecture	• Offered LTO-8 drive in the Library shall conform to the Data rate matching technique for higher reliability • Tape Drive Architecture in the Library shall conform to the INCITS/T10 SCSI-3 standard or newer standards.
4	Scalability	• Tape Library shall be scalable to minimum of 21 number of LTO-8 drives
5	Speed	• Offered LTO-8 drive shall support 300MB/sec in Native mode.
6	Connectivity	• Offered Tape Library shall provide native FC connectivity to SAN switches.
7	Partitioning	• Offered tape library shall have flexibility to configure each offered drive into a separate partition. Offered tape library shall have support for 21 partition when fully populated.
8	Encryption device	• Offered Library shall be provided with a hardware device like USB key, separate appliance etc. to keep all the encrypted keys in a redundant fashion.

9	Management	• Tape Library shall provide web based remote management.
10	Barcode Reader and Mail slots	• Tape library shall support Barcode reader and mail slot • Tape Library shall be offered with 5 mail slots and shall be scalable to 30 slots when fully populated. • Offered LTO-8 drive shall also support LTO-7 – Type M media so that native cartridge capacity of LTO-7 cartridge can be increased to 9TB.
11	Other Features	• Tape Library shall have GUI Panel • Shall be rack mountable • Should have redundant power supply • Tape Library shall be supplied with software which can predict and prevent failures through early warning and shall also suggest the required service action • Offered drives in the tape library shall optionally support both data path and control path failover • Offered Software shall also have the capability to determine when to retire the tape cartridges and what compression ratio is being achieved
12	Warranty	• 5 Years 24x7 onsite support with commitment to resolve the problem within 6 Hours. Support has to be provided directly by OEM during the warranty period
13	Bill of Materials	• The vendor shall give part nos. of every component which will be cross verified by OEM
14	Manufacturer Authorization Letter	• Manufacturers Authorization Letter Specific to this tender must be submitted. Tender submitted without MAF will be rejected.

c) *Backup Software for DC & DR*

Sl. No.	Item	Description
1	Backup Software	• The proposed backup solution should be available on various OS platforms such as Windows, Linux and UNIX platforms. • The proposed backup solution shall support industry leading cluster solution such as MSCS, MC Service Guard, and Veritas Cluster. • The proposed backup software should support both backups using snapshot/hardware-based and software

		based as well as backup to tapes for long term and offline data retention.
		• The proposed backup software should automatically secure the communication between the server and the customer using Encrypted Control Communication.
		• The proposed backup software should support single management window for all the different data protection locations.
		• The proposed backup solution shall have same web-based GUI across heterogeneous platform to ensure easy administration.
		• The proposed backup solution should support tape mirroring of the same job running concurrently with primary backup.
		• The proposed backup software should use web-based scheduler for the backup jobs.
		• The proposed backup software should support the use REST API for browse and restore operations.
		• The proposed backup solution should allow creating tape clone facility after the backup process.
		• The proposed backup solution should allow creating tape clone facility after the backup process.
		• The proposed backup solution shall be configured in such a fashion that no extra license for customer and media servers is required while moving from LAN to SAN based backup.
		• Backup software licenses to be provided for the offered capacity of SAN Storage.

vi)   SAN Switches for DC & DR

a) *SAN Switches (DC) – 48 Ports*

Sl. No.	Description
1	**Accepted Make & Model: HPE/CISCO/Broadcom**
2	Minimum Dual SAN switches shall be configured where each SAN switch shall be configured 44 * 16Gbps ports on each switch and 4 * 8Gbps Long Wave SFP+ Ports

3	Should deliver 16 Gbit/Sec Non-blocking architecture with 1:1 performance for up to 48 ports in energy-efficient fashion
4	Should protect existing device investments with autosensing 4, 8, and 16 Gbit/sec capabilities.
5	The switch shall support different port types such as FL_Port, F_Port, E_Port, EX_Port.
6	The switch should be rack mountable
7	Should provide enterprise-class availability features such as redundant and hot pluggable components like power supply and FAN
8	The switch shall provide Aggregate bandwidth of 768 Gbit/sec end to end.
9	Switch shall have support for web-based management and should also support CLI.
10	The switch should have USB port for firmware download, support save, and configuration upload/download.
11	Offered SAN switches shall be highly efficient in power consumption.
12	Switch shall support POST and online/offline diagnostics, including trace logging, environmental monitoring, non-disruptive daemon/stateful process restart, FC ping and Pathinfo (FC traceroute), port mirroring (SPAN port).
13	Offered SAN switch shall support services such as Quality of Service (QoS) to help optimize application performance in consolidated, virtual environments. It should be possible to define high, medium and low priority QOS zones to expedite high-priority traffic
14	The switch shall be able to support ISL trunk up to 128 Gbit/sec between a pair of switches for optimal bandwidth utilization and load balancing.
15	SAN switch shall support to restrict data flow from less critical hosts at preset bandwidths.
16	It should be possible to isolate the high bandwidth data flows traffic to specific ISLs by using simple zoning
17	The Switch should be configured with the Zoning and shall support ISL Trunking features when cascading more than 2 numbers of SAN switches into a single fabric.
18	Offered SAN switches shall support to measure the top bandwidth-consuming traffic in real time for a specific port or a fabric which should detail the physical or virtual device.
19	5 Years 24x7 onsite support with commitment to resolve the problem within 6 Hours. Support has to be provided directly by OEM during the warranty period.
20	The vendor has to give make, model, part nos. of every component which will be cross verified by OEM.
21	Manufacturers Authorization Letter Specific to this tender must be submitted. Tender submitted without MAF will be rejected.

b) SAN Switches (DR) – 24 Ports

Sl. No.	Description
1	**Accepted Make & Model: HPE/CISCO/Broadcom**
2	Minimum Dual SAN switches shall be configured where each SAN switch shall be configured with 24 * 16Gbps FC Ports on each switch
3	Required scalability shall not be achieved by cascading the number of switches and shall be offered within the common chassis only
4	Should deliver 16 Gbit/Sec Non-blocking architecture with 1:1 performance for up to 24 ports in a energy-efficient fashion
5	Should protect existing device investments with auto-sensing 4, 8, and 16 Gbit/sec capabilities.
6	The switch shall support different port types such as FL_Port, F_Port, E_Port, EX_Port.
7	The switch should be rack mountable
8	Should provide enterprise-class availability features such as redundant and hot pluggable components like power supply and FAN
9	The switch shall provide Aggregate bandwidth of 384 Gbit/sec end to end.
10	Switch shall have support for web-based management and should also support CLI.
11	The switch should have USB port for firmware download, support save, and configuration upload/download.
12	Offered SAN switches shall be highly efficient in power consumption.
13	Switch shall support POST and online/offline diagnostics, including trace logging, environmental monitoring, non-disruptive daemon/ stateful restart, FCping and Pathinfo (FC traceroute), port mirroring (SPAN port).
14	Offered SAN switch shall support services such as Quality of Service (QoS) to help optimize application performance in consolidated, virtual environments. It should be possible to define high, medium and low priority QOS zones to expedite high-priority traffic
15	The switch shall be able to support ISL trunk up to 128 Gbit/sec between a pair of switches for optimal bandwidth utilization and load balancing.
16	SAN switch shall support to restrict data flow from less critical hosts at preset bandwidths.
17	It should be possible to isolate the high bandwidth data flows traffic to specific ISLs by using simple zoning
18	The Switch should be configured with the Zoning and shall support ISL Trunking features when cascading more than 2 numbers of SAN switches into a single fabric.

19	Offered SAN switches shall support to measure the top bandwidth-consuming traffic in real time for a specific port or a fabric which should detail the physical or virtual device.
20	5 Years 24x7 onsite support with commitment to resolve the problem within 6 Hours. Support has to be provided directly by OEM during the warranty period.
21	The vendor has to give make, model, part nos. of every component which will be cross verified by OEM.
22	Manufacturers Authorization Letter Specific to this tender must be submitted. Tender submitted without MAF will be rejected.

vii)   Core Switches (DC and DR)

Sl. No.	Description	
1	**Accepted Make & Model: HPE/CISCO/Extreme**	
2	Form Factor	Chassis switch with Minimum 4 usable Slots 19 Inch Rack mountable switch with management/supervisor Engine 1+1. OEM should provide all the hardware including fabric cards, CPU, Power Supplies, Fan Trays etc. and software, licenses to get full capacity of the provided chassis.
3	Architecture	Non-Blocking architecture. Must have EAL3 /NDCPP or above common criteria certification.
4	IPV6 Compliance	All Functionalities of Switch shall be IPV4 and IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software.
5	End of sale	OEM End-of-sale declaration shall not have been released for the quoted model at the time of the bid submission.
6	Feature Availability	All the specified features/ parameters/ certifications must be available on the Technical Bid opening date. Features/ parameters/ certifications proposed to be available in near future/ on roadmap shall not be considered. Switch should support ISSU (In Service Software upgrade), Virtualization, Fabric provisioning support BGP-EVPN, OSPF VxLAN, VRF, VRRP Should support VM-aware Network Automation, Should support 802.1Qbb, netconf, openstack/ openflow/ REST API support in same hardware.
7	Ports	48 port 1/10G SFP+ populated with 24 Nos SFP+ multimode transceivers and Switch should have 40/100 Gbps ports module cards scalability in same hardware from day 1.

8	SFP Transceivers	All the Transceivers/Modules used to connect the Switches should be from the same OEM/make of the switches only. Switch should support 1Gbps and 10Gbps models.
Hardware Specification		
1	Centralized wire capacity	switch at least 9.6 Tbps switching bandwidth or more
2	Per Slot Switching Capacity	2.4 Tbps
3	Total number of IPv4 routes	Total number of IPv4 routes 112000 or more,
4	VLANs (802.1q tagged VLAN)	4000 or more Concurrent
5	Memory	8GB DRAM or more
6	Storage	At least 1 GB SSD/Flash
Support		
1	Switches must be supported for a minimum of 5 years by the hardware vendor with software updates and upgrades without additional cost.	
2	The OEM should provide support services 24x7 TAC with L1, L2 and L3 for 5 years free of cost. India toll free number should be reflected in official website of the OEM. Hardware replacement support should be 6 Hrs.	

viii)   TOR Switches for DC & DR

Sl. No.	Description
Accepted Make & Model: HPE/ CISCO/ EXTREME	
1	**Architecture**
1.1	The switch should have at least 24 * SFP+ ports Loaded with 24*10G SR transceivers and 4 QSFP+ Ports
1.2	The switch should support dual power supply and fan tray
1.3	The switch should have Minimum of 1GB flash/SD RAM/DDRAM/SSD
1.4	At least 960 Gbps switching capacity
1.5	MAC Address table size of 128,000 entries
1.6	The Switch should have modular operating system
2	**Quality of Service** (QoS)

2.1	The switch should support IEEE 802.1p precedence
2.2	The Switch should support Strict Priority SP, WRR or equivalent feature.
3	**Data Center optimized**
3.1	The switch should support virtualization/stacking. Stacking cables to be provided
3.2	The switch should support for IEEE 802.1Qbb Priority Flow Control (PFC), Data Center Bridging Exchange (DCBX), or equivalent
4	**Manageability**
4.1	The switch should provide CLI capabilities
4.2	The switch should support Port monitoring capabilities
4.3	The switch should support Traceroute and ping functionality
4.4	The switch should support Multiple configuration files
4.5	The switch should support sFlow (RFC 3176) or equivalent
4.6	The switch should support SNMP v1, v2c and v3 or equivalent
4.7	The switch should support Out-of-band interface functionality
4.8	The switch should support Remote configuration and management capability
4.9	The switch should provide configuration via DHCP protocol
4.10	The switch should support Network Time Protocol (NTP)/Secure Network Time Protocol (SNTP)/Precision Time Protocol (PTP) RFC 1855 Compliant
4.11	The switch should support Device Link Detection Protocol (DLDP) or equivalent
4.12	The switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) or equivalent
5	**Layer 2 switching**
5.1	The switch should support 4,094 VLANs based on port. VLAN Mapping
5.2	The switch should provide full DHCP relay features with DHCP Snooping support
6	**Layer 3 routing**
6.1	The switch should support Equal-Cost Multipath (ECMP) feature
6.2	The switch should support routing of IP static routes, RIP, OSPF, and BGP from day 1
6.3	The switch should be able to separate stacks for IPv4 and IPv6
7	**Software Defined Networking (SDN) Capability**
7.1	OpenFlow or equivalent protocol to enable software-defined networking
7.2	Allows the separation of data (packet forwarding) and control (routing decision) paths, to be controlled by an internal/external SDN Controller
8	**Security**

8.1	The switch should provide IP Layer 3 filtering capability based on source/destination IP address/subnet and source/destination TCP/UDP port number.
8.2	The switch should support IEEE 802.1X and RADIUS/TACACS network login
8.3	The switch should allow access only to specified MAC addresses, which can be learned or specified by the administrator
9	**Environmental Features**
9.1	Switch should be ROHS Compliance
9.2	Switch should support AC/DC Power inputs
9.3	Operating temperature of 0°C to 40°C
10	**Warranty & MAF**
10.1	5 Years 24x7 onsite support with commitment to resolve the problem within 6 Hours of the point of problem detection. Support have to be provided directly by OEM during the warranty period.
10.2	The vendor has to give make, model, part nos. of every component which will be cross verified by OEM.
10.3	Manufacturers Authorization Letter Specific to this tender must be submitted. Tender submitted without MAF will be rejected.

ix)   1G Switch (DC & DR)

a) *1G Switch (DC & DR) – Type 1*

Sl. No.	Description
Accepted Make & Model: Cisco/ Extreme/ HPE	
1	**Architecture**
1.1	Shall be 1RU, 19" Rack Mountable
1.2	48 RJ-45 autosensing 10/100/1000 ports
1.3	The switch shall support 2*10-Gigabit ports SFP+ and 2 RJ-45 1/10GBASE-T ports in addition to the above ports
1.4	Switch should have 1 RJ-45 serial console port
1.5	Switch should have switching capacity of 176 Gbps
1.6	Switch should provide 10/100/1G ports
1.7	Switch should support 16000 MAC address
2	**Management**
2.1	The Switch should support Intuitive Web browser-based management and Command Line Interface (CLI) capabilities

2.2	The Switch should support Secure Web-management sessions with HTTPS / SSL
2.3	The Switch should support SNMPv1, v2c, and v3 protocols
2.4	The Switch should support Port mirroring feature
2.5	The Switch should support Network Time Protocol (NTP) capability
2.6	The Switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) or equivalent protocol
2.7	The Switch should support RMON capability
2.8	The Switch should support DHCP client modes
3	**Quality of Service (QoS)**
3.1	The Switch should support Broadcast control to allows limitation of broadcast traffic rate to cut down on unwanted network broadcast traffic
3.2	The Switch should support Rate limiting to sets per-port enforced maximums and per-port, per-queue minimums
3.3	The Switch should support Traffic prioritization and at least four hardware queues
4	**Connectivity**
4.1	The Switch should support IEEE 802.3X flow control
4.2	The Switch should support Packet storm protection to protects against broadcast, multicast, or unicast storms with user-defined thresholds
4.3	The Switch should support IPv6 host to enable switches to be managed and deployed at the IPv6 network's edge
4.4	The Switch should support IPv6 static routes
4.5	The Switch should support MLD snooping to forwards IPv6 multicast traffic to the appropriate interface, preventing traffic flooding
4.6	The Switch should support ACL and QoS for IPv6 network traffic
5	**Security**
5.1	The Switch should support IEEE 802.1X and RADIUS/TACACS network logins to controls port-based access for authentication and accountability
5.2	The Switch should support Automatic VLAN assignment to assign users automatically to the appropriate VLAN based on their identity, location and time of day
5.3	The Switch should support STP BPDU port protection to blocks Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs
5.4	The Switch should protect the root bridge from malicious attacks or configuration mistakes
5.5	The Switch should support Automatic denial-of-service protection to protects the network by blocking malicious DoS attacks aimed at the switch itself.

5.6	The Switch should provide security so that only authorized access to the Web browser interface is allowed
6	**Performance**
6.1	The Switch should support IGMP / MLD Snooping to improve network performance by filtering multicast traffic when there is no multicast receiver on a connection.
7	**Layer 2 switching**
7.1	The Switch should support IEEE 802.1Q with 4,000 simultaneous VLAN IDs
7.2	The Switch should support standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) or equivalent protocols
7.3	The Switch should support BPDU filtering to improve network efficiency by filtering unnecessary BPDU packets on a port.
8	**Layer 3 services**
8.1	The Switch should support DHCP relay
9	**Layer 3 routing**
9.1	The Switch should support Static IPv4/IPv6 routing
10	**Resiliency and high availability**
10.1	The Switch should support stacking and create a single logical managed unit with up to four switches
10.2	The Switch should support Link aggregation to groups together up to 8 ports per trunk automatically using Link Aggregation Control Protocol (LACP), or manually, to form an ultra-high-bandwidth connection to the network backbone.
11	**Convergence**
11.1	The Switch should support LLDP-MED (Media Endpoint Discovery)
11.2	The Switch should support Auto voice VLAN to recognize IP phones and automatically assigns voice traffic to dedicated VLAN for IP phones
12	**Environmental Features**
12.1	Shall provide support for RoHS regulations
12.2	Switch should support operating temperature of 0°C to 40°C
12.3	Switch should comply with Safety and Emission standards
13	**Warranty & MAF**
13.1	5 Years 24x7 onsite support with commitment to resolve the problem within 6 Hours. Support has to be provided directly by OEM during the warranty period.
13.2	The vendor has to give make, model, part nos. of every component which will be cross verified by OEM.

Sl. No.	Description
13.3	Manufacturers Authorization Letter Specific to this tender must be submitted. Tender submitted without MAF will be rejected.

b)   1G Switch (DC) – Type 2

SI. No.	Description
Accepted Make & Model: Cisco/ Extreme/ HPE	
1	**Architecture**
1.1	Shall be 1RU, 19" Rack Mountable
1.2	24 RJ-45 autosensing 10/100/1000 ports
1.3	The switch should support 2*10-Gigabit ports SFP+ loaded with 2*SR transceivers and 2 RJ-45 1/10GBASE-T ports in addition to the above ports
1.4	Switch should have 1 RJ-45 serial console port
1.5	Switch should have switching capacity of 128 Gbps
1.6	Switch should support 16000 MAC address
2	**Management**
2.1	The Switch should support Intuitive Web browser-based management and Command Line Interface (CLI) capabilities
2.2	The Switch should support Secure Web-management sessions with HTTPS / SSL
2.3	The Switch should support SNMPv1, v2c, and v3 protocols
2.4	The Switch should support Port mirroring feature
2.5	The Switch should support Network Time Protocol (NTP) capability
2.6	The Switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
2.7	The Switch should support RMON capability
2.8	The Switch should support DHCP client modes
3	**Quality of Service (QoS)**
3.1	The Switch should support Broadcast control to allows limitation of broadcast traffic rate to cut down on unwanted network broadcast traffic
3.2	The Switch should support Traffic prioritization and at least 8 hardware queues
4	**Connectivity**
4.1	The Switch should support IEEE 802.3X flow control
4.2	The Switch should support Packet storm protection to protects against broadcast, multicast, or unicast storms with user-defined thresholds
4.3	The Switch should support Jumbo frame up to 9-kilobyte frames

4.4	The Switch should support IPv6 host to enable switches to be managed and deployed at the IPv6 network's edge
4.5	The Switch should support IPv6 static routes
4.6	The Switch should support MLD snooping to forwards IPv6 multicast traffic to the appropriate interface, preventing traffic flooding
4.7	The Switch should support ACL and QoS for IPv6 network traffic
5	**Security**
5.1	The Switch should support IEEE 802.1X and RADIUS/TACACS network logins to controls port-based access for authentication and accountability
5.2	The Switch should support Automatic VLAN assignment to assign users automatically to the appropriate VLAN based on their identity, location and time of day
5.3	The Switch should support STP BPDU port protection to blocks Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs
5.4	The Switch should support Automatic denial-of-service protection to protects the network by blocking malicious DoS attacks aimed at the switch itself.
5.5	The Switch should provide security so that only authorized access to the Web browser interface is allowed
6	**Performance**
6.1	The Switch should support IGMP / MLD Snooping to improve network performance by filtering multicast traffic when there is no multicast receiver on a connection.
7	**Layer 2 switching**
7.1	The Switch should support IEEE 802.1Q with 4,000 simultaneous VLAN IDs
7.2	The Switch should support standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) or equivalent protocols
7.3	The Switch should support BPDU filtering to improve network efficiency by filtering unnecessary BPDU packets on a port.
8	**Layer 3 services**
8.1	The Switch should support DHCP relay
9	**Layer 3 routing**
9.1	The Switch should support Static IPv4/IPv6 routing
9.2	The Switch should support 8 virtual VLAN interfaces as a minimum
10	**Resiliency and high availability**

10.1	The Switch should support stacking and create a single logical managed unit with up to four switches
10.2	The Switch should support Link aggregation to groups together up to 8 ports per trunk automatically using Link Aggregation Control Protocol (LACP), or manually, to form an ultra-high-bandwidth connection to the network backbone. The switch should provide support up to 128 trunks
11	**Convergence**
11.1	The Switch should support LLDP-MED (Media Endpoint Discovery)
11.2	The Switch should support Auto voice VLAN to recognize IP phones and automatically assigns voice traffic to dedicated VLAN for IP phones
12	**Environmental Features**
12.1	Shall provide support for RoHS regulations
12.2	Shall have features to improve energy efficiency like variable-speed fans
12.3	Switch should support operating temperature of 0°C to 40°C
12.4	Switch should support safety and emission standards.
13	**Warranty & MAF**
13.1	5 Years 24x7 onsite support with commitment to resolve the problem within 6 Hours. Support has to be provided directly by OEM during the warranty period.
13.2	The vendor has to give make, model, part nos. of every component which will be cross verified by OEM.
13.3	Manufacturers Authorization Letter Specific to this tender must be submitted. Tender submitted without MAF will be rejected.

x)   Local Hardware at Plant Locations

a) XMII Rack Servers

SI. No.	Item	Description
1	**Make & Model**	**Accepted Make & Model: HPE/ DELL/ CISCO**
2	Chassis	2 U Rack Mountable
3	CPU	2x Intel Xeon-Gold 6246 (3.3GHz/12-core/165W) Processor
4	Memory	24DIMM slots. 384 (12x32GB DIMM) GB Dual Rank RDIMMs
5	Hard disk drive	2x 600GB SAS 10K RPM & 6 x 1.2TB 10K RPM SAS drives

b) ADS, Antivirus & Patch Mgmt Servers (Rack Server)

Sl. No.	Item	Description
1	**Make & Model**	**Accepted Make & Model: HPE/ DELL/ CISCO**
2	Chassis	2 U Rack Mountable
3	CPU	2x Intel Xeon-Gold 6234 (3.3GHz/8-core) Processor
4	Memory	24DIMM slots. 192 (6x32) GB Dual Rank RDIMMs
5	Hard disk drive	3 x 1.2TB 10K RPM SAS drives

c) Other General Specifications

Sl. No.	Item	Description
1	Memory Protection	ECC with multi-bit error protection, Online spare or mirrored memory
2	HDD Bays	Up to 8 SFF HDD/SSD
3	Controller	It should support Integrated or add-on PCIe 3.0 based 12G SAS Raid Controller with RAID 0, 1, 5, 6, 10, 50, 60 with 2GB of Flash backed write cache onboard
4	Networking features	1Gb 4-port network adaptors 2x10Gb 2-port adapter 10GBASET Copper (adapter level fault tolerance is required)
5	Interfaces	Serial – 1 Micro SD slot – 1 USB 3.0 support With Up to 5 Total:
6	Bus Slots	Server should support three PCI-Express 3.0 slots, at least one x16 PCIe slots
7	Power Supply	Should support hot plug redundant power supplies with minimum 94% efficiency
8	Fans	Redundant hot-plug system fans

9	Industry Standard Compliance	ACPI 4.0 Compliant or above
		PCIe 3.0 Compliant
		PXE Support
		Energy Star
		ASHRAE A3/A4 or later
		SMBIOS Redfish API
		SNMP v3
		TLS 1.2
		DMTF Systems Management Architecture
10	System Security	UEFI Secure Boot and Secure Start support
		Security feature to ensure servers do not execute compromised firmware code
		FIPS 140-2 validation
		Common Criteria certification
		Configurable for PCI DSS compliance
		Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser or equivalent
		Tamper-free updates - components digitally signed and verified
		Secure Recovery - recover critical firmware to known good state on detection of compromised firmware
		Ability to rollback firmware
		Secure erase of NAND/User data
		TPM (Trusted Platform Module) 1.2
		TPM (Trusted Platform Module) 2.0
		Configurable for PCI DSS compliance
		Secure erase of NAND
		Chassis Intrusion detection
11	Operating Systems and Virtualization Software Support	Microsoft Windows Server
		Red Hat Enterprise Linux for SAP (RHEL)
		SUSE Linux Enterprise Server for SAP (SLES)
		VMware
12	GPU support	System should support NVIDIA's latest computational accelerators and graphics accelerators

13	System Performance Tuning	1. System should support feature for improved workload throughput for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode without the frequency fluctuations associated with running in turbo mode
		2. System should support workload Profiles for simple performance optimization
14	Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable
		2. Should maintain repository for firmware and drivers' recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware
15	Server Management	System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive.
		System should support embedded remote support to transmit hardware events directly to OEM for automated phone home support
		Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD and automatic calls logging. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support.
		Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contracts and status. The Portal should also provide a personalized dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).
		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.
		The Server Management Software should be of the same brand as of the server supplier.

16	Cloud Enabled Monitoring and Analytics or equivalent web console.	1. Offered servers shall have cloud enabled monitoring for proactive management. All required licenses for same shall be included in the offer. 2. Cloud Enabled Monitoring shall have capability to provide following: a. Providing Firmware upgrade and patch upgrade recommendations proactively. b. Providing power and support entitlement status. c. Recommendations to eliminate performance bottlenecks and critical events, having capability of proactive recommendation for arresting the issues / problems.
17	Warranty	5 Years 24x7 onsite support with commitment to resolve the problem within 6 Hours. Support has to be provided directly by OEM during the warranty period.
18	Bill of Materials	The vendor has to give make, model, part nos. of every component which will be cross verified by OEM.
19	Manufacturer Authorization Letter	Manufacturers Authorization Letter Specific to this tender must be submitted. Tender submitted without MAF will be rejected.

2.2. DC & DR Software

i) Enterprise Management System (EMS) Solution (DC & DR)

Sl. No.	Description
Make & Model: Any Reputed Make	
General Requirement – For Entire NMDC Network	
1	The proposed EMS solution should be an integrated, modular and scalable solution from single OEM (i.e. all Network Monitoring, server Monitoring including application and database monitoring and Service Management tools should be from single OEM) to provide comprehensive fault management, performance management, traffic analysis and business service management, IT service desk\ help desk \trouble ticketing system & SLA monitoring functionality.
2	It should have a secured single sign-on and unified console for all functions of components offered for seamless cross-functional navigation & launch for single pane of glass visibility across multiple areas of monitoring & management.
3	The proposed EMS solution should be built on modern container technologies and have an option to deploy on classic mode non-containerized as well as containerized mode.

4	The solution should have self-monitoring ability to track status of its critical components & parameters such as Up/Down status of its services, applications & servers, CPU utilization, Memory capacity, File system space, Database Status, synchronization status between primary and secondary system and event processing etc. It should provide this information in real-time through graphical dashboards, events/alarms as well as in the form of historical reports.
5	To ensure the proposed software is secure, it should have ISO 27034 certification from a verification or certification agency which has global recognition.
6	EMS/NMS OEM must be an industry standard, enterprise grade solution and shall be in the present in Gartner's MQ reports for NPMD and ITSM for last two years (2017 & 2018).
7	It shall be ensured by MSP/OEM that the proposed EMS solution (hardware and software) provisioned from Day 1 is able to handle 3000 devices and shall be scalable to 5000 devices.
8	Proposed EMS Solutions MUST have been in operations in at least 3 or more deployments across government/public sector, monitoring and managing at least 10,000 network nodes in each of the cases individually. Self-certification of the OEM, along with the customer names and proof of software delivery must be submitted at the time of bid submission.
9	Solution should ensure compatibility of existing Infrastructure with the procured infrastructure and it must fill the end functionality of the project. Offered solution should support bi-directional integration between the NOC and SOC to have the single consolidated console of infrastructure and security events.
Server Fault Monitoring & Application Performance Management	
10	The proposed Enterprise Management tools must be able to monitor end to end performance of Server Operating Systems & Databases and Should be able to manage distributed, heterogeneous systems – Windows, UNIX & LINUX from a single management station.
11	Should provide a centralized point of control with out-of-the-box policy-based management intelligence for easy deployment for the servers, operating systems, applications and services for correlating and managing all the IT infrastructure components of a business service
12	There should be a single agent on the managed node that provides the system performance data, and for event management it should be able to prioritize events, do correlation & duplicate suppression ability to buffer alarms and provide automatic actions with capability to add necessary annotations
13	Each operator should be provided with user roles that should include operational service views enabling operators to quickly determine impact and root cause associated with events.
14	The system should integrate with Helpdesk / Service desk tool for automated incident logging and also notify alerts or events via e-mail or SMS.

15	The system should have context-based analysis and forecasting based on performance data with automated policy deployment with detailed, intelligent monitoring of performance and availability data collection
16	Solution should provide alarm correlation and facilitate reduction of total number of alarms displayed by means of intelligent alarm correlation, suppression and root cause analysis techniques built into the system. The system must ensure reduction in MTTR by means of advanced event correlation, filtering and root cause analysis.
17	The proposed Alarm Correlation and Root Cause Analysis system shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network components. The current performance state of the entire network & system infrastructure shall be visible in an integrated console.
18	It should have capability to perform cross domain correlation with alarm correlation from Network Monitoring tool, Systems monitoring tool and other domain monitoring tools.
19	Alarm Filtering should allow flexible filtering rules for DC staff to filter the alarms by category, severity, elements, duration, by user, by views, by geography or by department.
20	The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis.
21	Should be able to send e-mail or Mobile –SMS to pre-defined users for pre-defined faults.
22	The proposed solution should able to monitor application middleware & database
Network Fault Monitoring & Performance Management with Reporting	
23	The Network Management function must monitor performance across heterogeneous networks from one end of the enterprise to the other.
24	The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time; in order to keep the topology always up to date. This discovery should run at a low overhead, incrementally discovering devices and interfaces.
25	The tool should automatically discover different type of heterogeneous devices (all SNMP supported devices i.e. Router, Switches, LAN Extender, Servers, Terminal Servers, Thin-Customer and UPS etc.) and map the connectivity between them with granular visibility up to individual ports level. The tool shall be able to assign different icons/ symbols to different type of discovered elements. It should show live interface connections between discovered network devices.
26	It should support various discovery protocols to perform automatic discovery of all L2, L3 Network devices across NMDC locations and any further Network connectivity's planned in future.
27	The tool shall be able to discover IPv4 only, IPv6 only as well as devices in dual-stack. In case of dual stack devices, the system shall be able to discover and show both IPv4 and IPv6 IP addresses.

28	The tool shall be able to work on SNMP V-1, V-2c & V-3 based on the SNMP version supported by the device. It shall provide an option to discover and manage the devices/elements based on SNMP as well as ICMP.
29	The proposed Network Fault Management solution must support extensive discovery mechanisms and must easily discover new devices using mechanisms such as SNMP Trap based discovery. It must also allow for inclusion and exclusion list of IP address or devices from such discovery mechanisms
30	The proposed solution must provide a detailed asset report, organized by vendor name, device type, listing all ports for all devices. The Solution must provide reports to identify unused/dormant Network ports in order to facilitate capacity planning
31	The propose solution should have diagnostic analytics capability that able to visually correlate performance and configuration changes of all network issues.
Network Configuration Automation	
32	The system should be able to clearly identify configuration changes / policy violations/ inventory changes across multi-vendor network tool.
33	The system should support secure device configuration capture and upload and thereby detect inconsistent "running" and "start-up" configurations and alert the administrators.
34	The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements:
35	a) Capture running configuration; b) Capture start-up configuration; c) Upload configuration; d) Write start-up configuration; e) Upload firmware
36	The proposed fault management solution must able to perform "load & merge" configuration changes to multiple network devices
37	The proposed fault management solution must able to perform real-time or scheduled capture of device configurations
38	NMS should support 3-Dimensional Compliance Model - Configuration, Software, Running State
Reporting	
39	Reporting solution should be able to report on Service Level status of configured business service.
40	It should be able to collect and collate information regarding relationship between IT elements and business service, clearly showing how infrastructure impacts business service levels.
41	The solution should be user configurable for building additional reports.
42	Solution should be able to collect Key performance measurements and statistics from all network domains and store it. This data is to be used for evaluation of performance of the end to end network infrastructure/services.

43	The performance management system shall be able to collect and report data like:
44	a. Packet delay and packet loss
45	b. User bandwidth usage rate
46	d. Network availability rate
47	e. CPU usage rate
48	f. Input/output traffic through physical ports
49	g. Input/output traffic through logical ports
50	The Performance Management shall have user defined set of reports like:
51	a. Summary Reports for specific groups: Reports displaying per group of resources the group aggregations for a set of metrics (for example, per City, the maximum traffic or the total traffic).
52	b. Summary Reports for specific Resources: Reports displaying for a set of resources the period aggregations for the same set of metrics (for example, per interface, the maximum traffic over the day)
53	c. Detailed chart Reports: Reports displaying for one resource and the same set of metrics the values over the period (for example, the raw collected values for the day).
54	d. Resource Threshold Violation Reports: Reports displaying the resources for which a threshold was violated
55	c. Detailed chart Reports: Reports displaying for one resource and the same set of metrics the values over the period (for example, the raw collected values for the day).
56	d. Resource Threshold Violation Reports: Reports displaying the resources for which a threshold was violated.
General Requirement of IT Service/ Helpdesk	
57	Should able to support and handle large volume of incident, service requests, changes, etc.
58	Should have the feature to integrate with third party IVR or CTI
59	The porposed helpdesk should have splutions like : Incident management, Problem Management, Change Management, Knowledge Management, Service Level Management, Service Asset and Configuration management, Service Catalogue and Request Fulfilment, etc. The certification copies to be submitted.
60	The solution should provide to browse through CMDB which should offer powerful search capabilities for configuration items and services, enabling to quickly find CIs as well as their relationships to other CIs.
61	Tool Analytics should be completely configurable in terms of source data and results, enabling Process Managers and other IT Users to proactively identify trends that can be used to drive action. Multiple instances shall be allowed to be configured in different ways in different modules for different outcomes - for example one should be able to identify trends in one set of data and

	subsequently develop linkages with other data, or Analytics can run on top of reporting results to provide further insights from unstructured data.
62	The tool should have the knowledge management OOB – knowledge databases to support investigations, diagnoses, root cause analysis techniques, and creating / updating workarounds, temporary fixes and resolutions
63	The tool should allow the creation of different access levels (i.e. Read only, write, create, delete) to knowledge management system
64	The proposed helpdesk solution must support code less configuration of processes that can be upgraded seamlessly without the need to reconfiguration of processes.
65	Solution should support comprehensive SLA management platform
66	Must allow creating and applying various operational level parameters to Incidents, Requests, Changes, and Release management modules.
67	The application should have a predefined/customizable field to indicate & track the progress/status of the lifecycle of ticket(s).
68	The tool should provide an audit trail, tracking & monitoring for record information and updates from opening through fulfilment to closure for example: IDs of individuals or groups opening, updating & closing records; dates / times of status & activities updates, etc.
69	SI's must proposed a full fledges Service Level Management Solution that allows for tracking of various service level performances of IT Infrastructure and vendor performance.
70	The solution should support SLA violations alerts during the tracking period.
71	The solution should support managing and maintaining a full history of an SLA.
72	The solution must provide a flexible framework for collecting and managing service level templates including Service Definition, Service Level Metrics, Penalties and other performance indicators measured across infrastructure and vendors
Auto-Discovery and Inventory	
73	Discovery should work without requiring agent installation (that is, agent-less discovery) while discovery Layers 2 through Layers 7 of OSI model
74	Should use Industry-standard protocols such as WMI, SNMP, JMX, SSH to perform discovery without requiring the installation of an agent
75	Discovery system should have ability to modify out-of-box discovery scripts, create customized discovery scripts
76	The EMS must provide a common configuration management database that must have a single solution for discovery of networks devices, servers & desktops, using a common probe, that supports both agent-less and agent-based technologies using.
Warranty & MAF	
77	5 Years 24x7 online support

Sl. No	Description
78	The vendor has to give make, model, part nos. of every component which will be cross verified by OEM.
79	Manufacturers Authorization Letter Specific to this tender must be submitted. Tender submitted without MAF will be rejected.

2.3. Firewall

i) Firewall (DC) – Type 1

Sl. No	Description
Accepted Make: Fortinet/ Palo Alto/ Cisco	
General	
1	The Firewall OEM should be leaders in latest Gartner's Enterprise Firewall Magic Quadrant report.
2	The Firewall OEM should be ICSA Labs certified for Firewall and should be Common Criteria EAL 4 certified
3	OEM should be having recommended rating from NSS Lab's Next Generation Firewall from past 2 years
4	OS should be "IPv6 Phase II Ready" certified
Hardware	
5	The Firewall must be appliance based
6	Should support 16 or more gigabit RJ45 interfaces
7	Should have 4 nos. of 10G SFP+ slots populated with the transceivers and should have upgrade option for 2 nos. of 40G QSFP+ in future
8	Should have 1 console port (RJ45) and 1 or more Number of USB ports
Firewall Performance	
10	Should have Firewall throughputs of minimum 60 Gbps or more
11	IPSec VPN throughput should be 20 Gbps or more
12	FW throughput should be 8 Gbps with enterprise mix traffic
13	Threat protection throughput should be 6 Gbps with enterprise mix traffic
14	Must support at least 8,000,000 or more concurrent connections
15	Must support at least 400,000 or more new sessions per second processing.
16	Should Support Virtualization (ie Virtual Systems / Virtual Domains). Should be having 10 or more virtual system license from day one

	Firewall Features
17	Should support both "bridge mode" or "transparent mode" apart from the standard NAT mode
18	Should provide NAT functionality, including PAT. Should support NAT 66, NAT 64, DNS 64, Static NAT IPv4 to IPv6 and vice versa (VIP64 and VIP46) and IPv6-IPv4 tunnelling or dual stack.
19	Should support IPv4 & IPv6 policies
20	Provision to create secure zones / DMZ (i.e. Multi- Zone support)
21	Should support the standards based Multi-Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.
22	Should support VLAN tagging (IEEE 802.1q) in NAT/Route mode
23	Should support Static routing and Dynamic Routing (RIP, OSPF & BGP)
24	Should support Active-Active as well as Active- Passive redundancy.
25	Should support ISP Load balancing and Failover
26	Should support multi-path intelligence based on link quality criteria
27	Should support link performance check based on packet loss, latency & jitter
28	Should support WAN path controller providing high application performance
29	Should support application specific rules based on SLA strategy
30	Should support high performance deep packet inspection for application identification and control
	Authentication
31	Should support User-Group based Authentication (Identity based Firewalling) & Scheduling
32	Should support authentication servers – RADIUS, LDAP & Active Directory
33	Support for RSA SecureID or other Token based Products
	VPN
34	The VPN should be integrated with firewall and should be ICSA Labs certified for IPSec VPN
35	Should support protocols such as DES & 3DES, MD5, SHA-1, SHA-256 authentication, Diffie- Hellman Group 1, Group 2, Group 5, Group 14, Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm, The new encryption standard AES 128, 192 & 256
36	Should support minimum 2000 IPSec Site-to-Site and 5000 no of IPSec Site-to-Client VPN tunnels.
37	Should have integrated SSL VPN with license for 500 concurrent SSL VPN users
38	Should support Single Sign-On Bookmarks for SSL Web VPN
39	Should support Windows, Linux and MAC OS for SSL-VPN
40	Should support NAT within IPSec/SSL VPN tunnels

41	Should also support PPTP and L2TP over IPSec VPN protocols.
42	Should support Stateful failover for both Firewall and VPN sessions.
IPS	
43	Should have a built-in Signature and Anomaly based IPS engine on the same unit
44	Should have protection for 7000+ signatures
45	Able to prevent denial of service and distributed Denial of Service attacks.
46	Supports user-defined signatures (i.e., Custom Signatures) with Regular Expressions.
Application Control	
47	Should have Application control feature with 3000 or more application signatures
48	Should perform Traffic Shaping based on applications
49	Should control popular IM/P2P, proxy applications regardless of port/protocol
Gateway Antivirus	
50	The appliance should facilitate embedded anti-virus support
51	Gateway AV should be supported for real-time detection of viruses and malicious code for HTTP, HTTPS, FTP, SMTP, SMTPS, POP3 and IMAP protocols
52	should also include Botnet filtering and detecting and preventing Botnet command and control traffic
53	Should have configurable policy options. Possible to select traffic to scan for viruses
Management, Log & Reporting	
54	Firewall should support management either through GUI/CLI or through Central Management
55	Firewall should support logging to multiple syslog servers.
56	Log & Reporting should be a dedicated solution out of the Firewall
57	The log & reporting tool needs to be bundled or quoted along with the solution. The logging and analysis should either be an appliance or on a dedicated PC/ Server platform with 12 TB storage. The Executing Agency should take the responsibility of supplying the hardware and the OS with suitable warranty.
58	The solution should provide comprehensive security event logging, reporting

ii)   Firewall (DR & Perimeter) – Type 2

Sl. No	Description
General	
Accepted Make: Fortinet/ Palo Alto/ Cisco	

1	The Firewall OEM should be leaders in latest Gartner's Enterprise Firewall Magic Quadrant report.
2	The Firewall OEM should be ICSA Labs certified for Firewall and should be Common Criteria EAL 4 certified.
3	OEM should be having recommended rating from NSS Lab's Next Generation Firewall from past 2 years.
4	OS should be "IPv6 Phase II Ready" certified
Hardware	
5	The Firewall must be appliance based
6	Should support 8 or more gigabit RJ45 interfaces
7	Should have 2 no of 10G SFP+ slots populated with the transceivers
8	Should have 1 console port (RJ45) and 1 or more Number of USB ports
9	Should have internal storage of 200 GB SSD
Firewall Performance	
10	Should have Firewall throughputs of minimum 30 Gbps or more
11	IPSec VPN throughput should be 10 Gbps or more
12	NGFW throughput should be 8 Gbps with enterprise mix traffic
13	Threat protection throughput should be 6 Gbps with enterprise mix traffic
14	Must support at least 7,000,000 or more concurrent connections
15	Must support at least 400,000 or more new sessions per second processing.
16	Should Support Virtualization (ie Virtual Systems / Virtual Domains). Should be having 10 or more virtual system license from day one
Firewall Features	
17	Should support both "bridge mode" or "transparent mode" apart from the standard NAT mode
18	Should provide NAT functionality, including PAT. Should support NAT 66, NAT 64, DNS 64, Static NAT IPv4 to IPv6 and vice versa (VIP64 and VIP46) and IPv6-IPv4 tunneling or dual stack.
19	Should support IPv4 & IPv6 policies
20	Provision to create secure zones / DMZ (ie Multi- Zone support)
21	Should support the standards based Multi-Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.
22	Should support VLAN tagging (IEEE 802.1q) in NAT/Route mode
23	Should support Static routing and Dynamic Routing (RIP, OSPF & BGP)
24	Should support Active-Active as well as Active- Passive redundancy.

25	Should support ISP Load balancing and Failover
26	Should support multi-path intelligence based on link quality criteria
27	Should support link performance check based on packet loss, latency & jitter
28	Should support WAN path controller providing high application performance
29	Should support application specific rules based on SLA strategy
30	Should support high performance deep packet inspection for application identification and control
Authentication	
31	Should support User-Group based Authentication (Identity based Firewalling) & Scheduling
32	Should support authentication servers – RADIUS, LDAP & Active Directory
33	Support for RSA Secure ID or other Token based Products
VPN	
34	The VPN should be integrated with firewall and should be ICSA Labs certified for IPSec VPN
35	Should support protocols such as DES & 3DES, MD5, SHA-1, SHA-256 authentication, Diffie- Hellman Group 1, Group 2, Group 5, Group 14, Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm, The new encryption standard AES 128, 192 & 256
36	Should support minimum 200 IPSec Site-to-Site and 1000 no of IPSec Site-to-Client VPN tunnels.
37	Should have integrated SSL VPN with license for 500 concurrent SSL VPN users
38	Should support Single Sign-On Bookmarks for SSL Web VPN
39	Should support Windows, Linux and MAC OS for SSL-VPN
40	Should support NAT within IPSec/SSL VPN tunnels
41	Should also support PPTP and L2TP over IPSec VPN protocols.
42	Should support Stateful failover for both Firewall and VPN sessions.
IPS	
43	Should have a built-in Signature and Anomaly based IPS engine on the same unit
44	Should have protection for 7000+ signatures
45	Able to prevent denial of service and distributed Denial of Service attacks.
46	Supports user-defined signatures (i.e., Custom Signatures) with Regular Expressions.
Application Control	
47	Should have Application control feature with 3000 or more application signatures
48	Should perform Traffic Shaping based on applications

49	Should control popular IM/P2P, proxy applications regardless of port/protocol
Gateway Antivirus	
50	The appliance should facilitate embedded anti-virus support
51	Gateway AV should be supported for real-time detection of viruses and malicious code for HTTP, HTTPS, FTP, SMTP, SMTPS, POP3 and IMAP protocols
52	should also include Botnet filtering and detecting and preventing Botnet command and control traffic
53	Should have configurable policy options. Possible to select traffic to scan for viruses
Management, Log & Reporting	
54	Firewall should support management either through GUI/CLI or through Central Management
55	Firewall should support logging to multiple syslog servers.
56	Log & Reporting should be a dedicated solution out of the Firewall
57	The log & reporting tool needs to be bundled or quoted along with the solution. The logging and analysis should either be an appliance or on a dedicated PC/ Server platform. The Executing Agency should take the responsibility of supplying the hardware and the OS with suitable warranty.
58	The solution should provide comprehensive security event logging, reporting

iii)   Firewall – Web Application Filter

Sl. No.	Description
Accepted Make & Model: Fortinet, Radware, F5, Imperva	
1	Web application firewall should be appliance based and provide specialized application threat protection.
2	Should be ICSA Certified
3	Should protect against application-level attacks targeted at web applications.
4	Should provide protection against sophisticated threats like SQL injection and cross-site scripting
5	Should provide controls to prevent identity theft, financial fraud and corporate espionage.
6	Appliance should have unlimited application licenses.
7	Automatic signature update and install
8	Device should have Sub Millisecond Latency
9	Should deliver at least 250 Mbps of WAF throughput

10	Should have minimum 4 no's of 1G RJ45
11	Should support at-least 4 nos of 1GB SFP slots
12	Should have minimum 200 GB of Storage space
13	Should have dual power supply
14	Dual-stack support for both IPv4 to IPv6 and IPv6 to IPv4 communication.
15	The appliance should be able to perform in multiple modes such as Active mode, passive mode, Transparent mode, Reverse proxy mode,
16	Appliance should continuously track the availability of the Servers being protected.
17	Should have a suitable Web Vulnerability Scanner to detect existing vulnerabilities in the protected web applications.
18	Should have Data Leak Prevention module to analyse all outbound traffic alerting/blocking any credit card leakage and information disclosure
19	Provide controls to meet PCI compliance requirements for web application servers.
20	Should have controls for Anti Web Defacement and provide ability to check the authorized version of the website content.
21	The solution should offer an on-board Anti-Virus solution for blocking the virus/malware file uploads into the servers from outside and the database should be updated automatically.
22	Should enforce strict RFC compliance check to prevent attacks such as encoding attacks, buffer overflows and other application specific attacks.
23	Should support automatic signature updates to protect against known and potential application security threats.
24	Should support XML firewall capability with schema validation, XML Firewall, IPS and routing capabilities.
25	Should Include policies for network and application layer denial of service threats
26	Should support XML Application protection
27	Should have built in policies
28	Should support custom signatures
29	Provide ability to allow/ deny URL access
30	Ability to define different policies for different applications
31	Ability to create custom attack signatures or events
32	Ability to combine detection and prevention

33	Should protect certain hidden form fields.
34	Must provide ability to allow or deny a specific URL access.
35	WAF should support Normalization methods such as URL Decoding, Null Byte string, termination, converting back slash to forward slash character etc..
36	A given user must be enforced to follow a sequence of pages while accessing.
37	Should provide a statistical view on collected application traffic
38	Should have controls against Brute force attacks
39	should Detect brute force attack (repeated requests for the same resource) against any part of the applications
40	Custom brute force attack detection for applications that do not return 401.
41	Protection against SYN-flood type of attacks
42	Should be able to protect Cookie Poisoning and Cookie Tampering.
43	Must support multiple HTTP versions
44	Should support restricting the methods used.
45	Should support restricting the method exceptions.
46	Should validate header length, content length, Body length, Parameter length, body line length etc..
47	The device must be supported in reverse proxy mode
48	Appliance should be able to terminate SSL
49	Should Passively decrypt SSL
50	Client certificates should be supported in passive mode and active mode.
51	In termination mode, the backend traffic (i.e. the traffic from the WAF to the web server) can be encrypted via SSL
52	Should support High Availability in active /Passive, Configuration Sync modes.
53	WAF appliance should have application-aware load-balancing engine to distribute traffic and route content across multiple web servers.
54	The vulnerability scan should identify vulnerabilities such as XSS, SQL injection, Source code disclosure, HTTP Request Smuggling, Common web server vulnerabilities etc..
55	Solution should be capable of detecting and distinguishing two sets of Bots from the Internet: Known search engines, Bad robots (scanners, crawlers, spiders)
56	Must be able to scan the authenticated applications.

57	Should support exclusions in scanning by the administrator.
58	Should support Secure Administrative Access using HTTPS and SSH
59	Should support Role Based Access Control for Management
60	Should support multi-tenancy feature via administrative domains
61	Separate network interface for SSH/HTTPS access.
62	Ability to identify and notify system faults and loss of performance
63	Should support multiple log formats such as CSV, Syslog, TXT, etc.
64	Should be able to send logs to the existing log & report solution
65	Should support inbuilt Reporting and sending the report via E-Mail
66	Should support report formats in PDF, HTML, WORD etc..
67	Should generate comprehensive event reports

iv) Firewall (Perimeter) – Type 3

Sl. No	Description
Accepted Make: Fortinet/Palo Alto/ Cisco	
General	
1	The Firewall OEM should be leaders in latest Gartner's Enterprise Firewall Magic Quadrant report.
2	The Firewall OEM should be ICSA Labs certified for Firewall and should be Common Criteria EAL 4 certified
3	OEM should be having recommended rating from NSS Lab's Next Generation Firewall from past 2 years
4	OS should be "IPv6 Phase II Ready" certified
Hardware	
5	The Firewall must be appliance based
6	Should support 12 or more gigabit RJ45 interfaces
7	Should support 1 or more Number of USB ports
8	Should have 1 console port (RJ45)
9	Should have internal storage of 200 GB SSD
Firewall Performance	

10	Should have Firewall throughputs of minimum 6 Gbps or more
11	IPSec VPN throughput should be 3 Gbps or more
12	NGFW throughput should be 300 Mbps with enterprise mix traffic
13	Threat protection throughput should be 250 Mbps with enterprise mix traffic
14	Must support at least 1,500,000 or more concurrent connections
15	Must support at least 30,000 or more new sessions per second processing.
16	Should Support Virtualization (ie Virtual Systems / Virtual Domains). Should be having 5 or more virtual system license from day one
	Firewall Features
17	Should support both "bridge mode" or "transparent mode" apart from the standard NAT mode
18	Should provide NAT functionality, including PAT. Should support NAT 66, NAT 64, DNS 64, Static NAT IPv4 to IPv6 and vice versa (VIP64 and VIP46) and IPv6-IPv4 tunneling or dual stack.
19	Should support IPv4 & IPv6 policies
20	Provision to create secure zones / DMZ (ie Multi- Zone support)
21	Should support the standards based Multi-Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.
22	Should support VLAN tagging (IEEE 802.1q) in NAT/Route mode
23	Should support Static routing and Dynamic Routing (RIP, OSPF & BGP)
24	Should support Active-Active as well as Active- Passive redundancy.
25	Should support ISP Load balancing and Failover
26	Should support multi-path intelligence based on link quality criteria
27	Should support link performance check based on packet loss, latency & jitter
28	Should support WAN path controller providing high application performance
29	Should support application specific rules based on SLA strategy
30	Should support high performance deep packet inspection for application identification and control
Authentication	
31	Should support User-Group based Authentication (Identity based Firewalling) & Scheduling
32	Should support authentication servers – RADIUS, LDAP & Active Directory
33	Support for RSA Secure ID or other Token based Products
VPN	
34	The VPN should be integrated with firewall and should be ICSA Labs certified for IPSec VPN

35	Should support protocols such as DES & 3DES, MD5, SHA-1, SHA-256 authentication, Diffie- Hellman Group 1, Group 2, Group 5, Group 14, Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm, The new encryption standard AES 128, 192 & 256
36	Should support minimum 200 IPSec Site-to-Site and 1000 no of IPSec Site-to-Client VPN tunnels.
37	Should have integrated SSL VPN with license for 200 concurrent SSL VPN users
38	Should support Single Sign-On Bookmarks for SSL Web VPN
39	Should support Windows, Linux and MAC OS for SSL-VPN
40	Should support NAT within IPSec/SSL VPN tunnels
41	Should also support PPTP and L2TP over IPSec VPN protocols.
42	Should support Stateful failover for both Firewall and VPN sessions.
IPS	
43	Should have a built-in Signature and Anomaly based IPS engine on the same unit
44	Should have protection for 7000+ signatures
45	Able to prevent denial of service and distributed Denial of Service attacks.
46	Supports user-defined signatures (i.e., Custom Signatures) with Regular Expressions.
Application Control	
47	Should have Application control feature with 3000 or more application signatures
48	Should perform Traffic Shaping based on applications
49	Should control popular IM/P2P, proxy applications regardless of port/protocol
Gateway Antivirus	
50	The appliance should facilitate embedded anti-virus support
51	Gateway AV should be supported for real-time detection of viruses and malicious code for HTTP, HTTPS, FTP, SMTP, SMTPS, POP3 and IMAP protocols
52	should also include Botnet filtering and detecting and preventing Botnet command and control traffic
53	Should have configurable policy options. Possible to select traffic to scan for viruses
	Web Filtering
54	The appliance should facilitate embedded Web Content Filtering feature
55	Web content filtering solution should work independently without the need to integrate with External proxy server.
56	URL database should have 200 million or more URLs under more than 70 categories
57	Should be able to block different categories/sites based on User Authentication.

	Management, Log & Reporting
58	Firewall should support management either through GUI/CLI or through Central Management
59	Firewall should support logging to multiple syslog servers.
60	Log & Reporting should be a dedicated solution out of the Firewall
61	The log & reporting tool needs to be bundled or quoted along with the solution. The logging and analysis should either be an appliance or on a dedicated PC/ Server platform. The Executing Agency should take the responsibility of supplying the hardware and the OS with suitable warranty.
62	The solution should provide comprehensive security event logging, reporting

v)   Firewall (Server Farm) – Type 4

Sl. No	Description
General	
Accepted Make: Fortinet/Palo Alto/ Cisco	
1	The Firewall OEM should be leaders in latest Gartner's Enterprise Firewall Magic Quadrant report.
2	The Firewall OEM should be ICSA Labs certified for Firewall and should be Common Criteria EAL 4 certified
3	OEM should be having recommended rating from NSS Lab's Next Generation Firewall from past 2 years
4	OS should be "IPv6 Phase II Ready" certified
Hardware	
5	The Firewall must be appliance based
6	Should support 12 or more gigabit RJ45 interfaces
7	Should have 2 no of 10G SFP+ slots populated with the transceivers
8	Should support 1 or more Number of USB ports
9	Should have 1 console port (RJ45)
Firewall Performance	
10	Should have Firewall throughputs of minimum 10 Gbps or more
11	IPSec VPN throughput should be 5 Gbps or more
12	NGFW throughput should be 1 Gbps with enterprise mix traffic
13	Threat protection throughput should be 800 Mbps with enterprise mix traffic

14	Must support at least 1,500,000 or more concurrent connections
15	Must support at least 30,000 or more new sessions per second processing.
16	Should Support Virtualization (i.e. Virtual Systems / Virtual Domains). Should be having 5 or more virtual system license from day one

Firewall Features	
17	Should support both "bridge mode" or "transparent mode" apart from the standard NAT mode
18	Should provide NAT functionality, including PAT. Should support NAT 66, NAT 64, DNS 64, Static NAT IPv4 to IPv6 and vice versa (VIP64 and VIP46) and IPv6-IPv4 tunneling or dual stack.
19	Should support IPv4 & IPv6 policies
20	Provision to create secure zones / DMZ (ie Multi- Zone support)
21	Should support the standards based Multi-Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.
22	Should support VLAN tagging (IEEE 802.1q) in NAT/Route mode
23	Should support Static routing and Dynamic Routing (RIP, OSPF & BGP)
24	Should support Active-Active as well as Active- Passive redundancy.
25	Should support ISP Load balancing and Failover
26	Should support multi-path intelligence based on link quality criteria
27	Should support link performance check based on packet loss, latency & jitter
28	Should support WAN path controller providing high application performance
29	Should support application specific rules based on SLA strategy
30	Should support high performance deep packet inspection for application identification and control

Authentication	
31	Should support User-Group based Authentication (Identity based Firewalling) & Scheduling
32	Should support authentication servers – RADIUS, LDAP & Active Directory
33	Support for RSA Secure ID or other Token based Products

VPN	
34	The VPN should be integrated with firewall and should be ICSA Labs certified for IPSec VPN
35	Should support protocols such as DES & 3DES, MD5, SHA-1, SHA-256 authentication, Diffie- Hellman Group 1, Group 2, Group 5, Group 14, Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm, The new encryption standard AES 128, 192 & 256

36	Should support minimum 200 IPSec Site-to-Site and 1000 no of IPSec Site-to-Client VPN tunnels.
37	Should have integrated SSL VPN with license for 200 concurrent SSL VPN users
38	Should support Single Sign-On Bookmarks for SSL Web VPN
39	Should support Windows, Linux and MAC OS for SSL-VPN
40	Should support NAT within IPSec/SSL VPN tunnels
41	Should also support PPTP and L2TP over IPSec VPN protocols.
42	Should support Stateful failover for both Firewall and VPN sessions.
IPS	
43	Should have a built-in Signature and Anomaly based IPS engine on the same unit
44	Should have protection for 7000+ signatures
45	Able to prevent denial of service and distributed Denial of Service attacks.
46	Supports user-defined signatures (i.e., Custom Signatures) with Regular Expressions.
Application Control	
47	Should have Application control feature with 3000 or more application signatures
48	Should perform Traffic Shaping based on applications
49	Should control popular IM/P2P, proxy applications regardless of port/protocol
Gateway Antivirus	
50	The appliance should facilitate embedded anti-virus support
51	Gateway AV should be supported for real-time detection of viruses and malicious code for HTTP, HTTPS, FTP, SMTP, SMTPS, POP3 and IMAP protocols
52	should also include Botnet filtering and detecting and preventing Botnet command and control traffic
53	Should have configurable policy options. Possible to select traffic to scan for viruses
Web Filtering	
54	The appliance should facilitate embedded Web Content Filtering feature
55	Web content filtering solution should work independently without the need to integrate with External proxy server.
56	URL database should have 200 million or more URLs under more than 70 categories
57	Should be able to block different categories/sites based on User Authentication.
Management, Log & Reporting	
58	Firewall should support management either through GUI/CLI or through Central Management

59	Firewall should support logging to multiple syslog servers.
60	Log & Reporting should be a dedicated solution out of the Firewall
61	The log & reporting tool needs to be bundled or quoted along with the solution. The logging and analysis should either be an appliance or on a dedicated PC/ Server platform. The Executing Agency should take the responsibility of supplying the hardware and the OS with suitable warranty.
62	The solution should provide comprehensive security event logging, reporting

vi)   Firewall (PLC Network) – Type 5

Sl. No	Specification
Accepted Make: Fortinet/Palo Alto/ Cisco	
General	
1	The Firewall OEM should be leaders in latest Gartner's Enterprise Firewall Magic Quadrant report.
2	The Firewall OEM should be ICSA Labs certified for Firewall and should be Common Criteria EAL 4 certified
3	OEM should be having recommended rating from NSS Lab's Next Generation Firewall from past 2 years
4	OS should be "IPv6 Phase II Ready" certified
Hardware	
5	The Firewall must be appliance based with rack mount option
6	Should support 8 or more gigabit RJ45 interfaces
7	Should support 1 or more Number of USB ports
8	Should have 1 console port (RJ45)
Firewall Performance	
9	Should have Firewall throughputs of minimum 2 Gbps or more
10	IPSec VPN throughput should be 1 Gbps or more
11	NGFW throughput should be 200 Mbps with enterprise mix traffic
12	Threat protection throughput should be 150 Mbps with enterprise mix traffic
13	Must support at least 1,000,000 or more concurrent connections
14	Must support at least 30,000 or more new sessions per second processing.
15	Should Support Virtualization (ie Virtual Systems / Virtual Domains). Should be having 5 or more virtual system license from day one

Firewall Features

16	Should support both "bridge mode" or "transparent mode" apart from the standard NAT mode
17	Should provide NAT functionality, including PAT. Should support NAT 66, NAT 64, DNS 64, Static NAT IPv4 to IPv6 and vice versa (VIP64 and VIP46) and IPv6-IPv4 tunneling or dual stack.
18	Should support IPv4 & IPv6 policies
19	Provision to create secure zones / DMZ (ie Multi- Zone support)
20	Should support the standards based Multi-Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.
21	Should support VLAN tagging (IEEE 802.1q) in NAT/Route mode
22	Should support Static routing and Dynamic Routing (RIP, OSPF & BGP)
23	Should support Active-Active as well as Active- Passive redundancy.
24	Should support ISP Load balancing and Failover
25	Should support multi-path intelligence based on link quality criteria
26	Should support link performance check based on packet loss, latency & jitter
27	Should support WAN path controller providing high application performance
28	Should support application specific rules based on SLA strategy
29	Should support high performance deep packet inspection for application identification and control

Authentication

30	Should support User-Group based Authentication (Identity based Firewalling) & Scheduling
31	Should support authentication servers – RADIUS, LDAP & Active Directory
32	Support for RSA Secure ID or other Token based Products

VPN

33	The VPN should be integrated with firewall and should be ICSA Labs certified for IPSec VPN
34	Should support protocols such as DES & 3DES, MD5, SHA-1, SHA-256 authentication, Diffie- Hellman Group 1, Group 2, Group 5, Group 14, Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm, The new encryption standard AES 128, 192 & 256
35	Should support minimum 100 IPSec Site-to-Site and 500 no of IPSec Site-to-Client VPN tunnels.
36	Should have integrated SSL VPN with license for 50 concurrent SSL VPN users

37	Should support Single Sign-On Bookmarks for SSL Web VPN
38	Should support Windows, Linux and MAC OS for SSL-VPN
39	Should support NAT within IPSec/SSL VPN tunnels
40	Should also support PPTP and L2TP over IPSec VPN protocols.
41	Should support Stateful failover for both Firewall and VPN sessions.
IPS	
42	Should have a built-in Signature and Anomaly based IPS engine on the same unit
43	Should have protection for 7000+ signatures
44	Able to prevent denial of service and distributed Denial of Service attacks.
45	Supports user-defined signatures (i.e., Custom Signatures) with Regular Expressions.
Application Control	
46	Should have Application control feature with 3000 or more application signatures
47	Should perform Traffic Shaping based on applications
48	Should control popular IM/P2P, proxy applications regardless of port/protocol
Gateway Antivirus	
49	The appliance should facilitate embedded anti-virus support
50	Gateway AV should be supported for real-time detection of viruses and malicious code for HTTP, HTTPS, FTP, SMTP, SMTPS, POP3 and IMAP protocols
52	should also include Botnet filtering and detecting and preventing Botnet command and control traffic
53	Should have configurable policy options. Possible to select traffic to scan for viruses
Web Filtering	
54	The appliance should facilitate embedded Web Content Filtering feature
55	Web content filtering solution should work independently without the need to integrate with External proxy server.
56	URL database should have 200 million or more URLs under more than 70 categories
57	Should be able to block different categories/sites based on User Authentication.
Management, Log & Reporting	
58	Firewall should support management either through GUI/CLI or through Central Management
59	Firewall should support logging to multiple syslog servers.
60	Log & Reporting should be a dedicated solution out of the Firewall

SI. No.	Description	
61	The log & reporting tool needs to be bundled or quoted along with the solution. The logging and analysis should either be an appliance or on a dedicated PC/ Server platform. The Executing Agency should take the responsibility of supplying the hardware and the OS with suitable warranty.	
62	The solution should provide comprehensive security event logging, reporting	

2.4. Switch, EMS

i) Core Switches for Site Locations

a) *Core Switch – Type 1*

SI. No.	Description	
1	Form Factor	Chassis switch with Minimum 4 usable Slots 19 Inch Rack mountable switch with management/supervisor Engine 1+1 availability. OEM should provide all the hardware including fabric cards, CPU, Power Supplies, Fan Trays etc. and software, licenses to get full capacity of the provided chassis.
2	Architecture	Non-Blocking architecture. Must have EAL3 /NDCPP or above common criteria certification.
3	IPV6 Compliance	All Functionalities of Switch shall be IPV4 and IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software.
4	End of sale	OEM End-of-sale declaration shall not have been released for the quoted model at the time of the bid submission.
5	Feature Availability	All the specified features/parameters/certifications must be available on the Technical Bid opening date. Features /parameters /certifications proposed to be available in near future / on roadmap shall not be considered. Switch should support ISSU (In Service Software upgrade), Virtualization, Fabric provisioning support BGP-EVPN, OSPF VxLAN, VRF, VRRP Should support VM-aware Network Automation, Should support Migration of Port Profiles or equivalent, Should support 802.1Qbb, netconf, openstack/ openflow, REST API support in same hardware.
6	Ports	24 Port 10G SFP Line Card, 24 Port 1G SFP Line card and 48 Port Copper 1G/10G Ports – each or 48 port

		1/10G SFP+. Switch should support 40/100 Gbps ports module cards scalability in same hardware from day 1.
7	SFP Transceivers	All the Transceivers/Modules used to connect the Switches should be from the same OEM/ make of the switches only. Switch should support 1Gbps and 10Gbps models.
Hardware Specification		
1	Centralized wire capacity	Switch at least 14 Tbps switching bandwidth or more
2	Per Slot Switching Capacity	3.2 Tbps or more
3	Total number of IPv4 routes	Total number of IPv4 routes 112000 or more,
4	VLANs (802.1q tagged VLAN)	4000 or more Concurrent
5	Memory	8GB DRAM or more
6	Storage	4GB SSD/Flash or more
Support		
1	Switches must be supported for a minimum of 5 years by the hardware vendor with software updates and upgrades without additional cost.	
2	The OEM should provide support services 24x7 TAC with L1, L2 and L3 for 5 years free of cost. India toll free number should be reflected in official website of the OEM.	

b) Core Switch – Type 2

SI. No.	Description	
1	Form Factor	Chassis switch with Minimum 4 usable Slots 19 Inch Rack mountable switch with management/supervisor Engine 1+1 availability. OEM should provide all the hardware including fabric cards, CPU, Power Supplies, Fan Trays etc. and software, licenses to get full capacity of the provided chassis.
2	Architecture	Non-Blocking architecture. Must have EAL3 /NDcPP or above common criteria certification.

3	IPV6 Compliance	All Functionalities of Switch shall be IPV4 and IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software.
4	End of sale	OEM End-of-sale declaration shall not have been released for the quoted model at the time of the bid submission.
5	Feature Availability	All the specified features/ parameters/ certifications must be available on the Technical Bid opening date. Features/ parameters/ certifications proposed to be available in near future/ on roadmap shall not be considered. Switch should support ISSU (In Service Software upgrade), Virtualization, Fabric provisioning support BGP-EVPN, OSPF VxLAN, VRF, VRRP Should support VM-aware Network Automation, Should support Migration of Port Profiles or equivalent, Should support 802.1Qbb, netconf, openstack/ openflow, REST API support in same hardware
6	Ports	24 Port 1G/10G SFP Line Card or 48 ports 1/10 Gbps SFP+ line card. Switch should support 40/100 Gbps ports module cards scalability in same hardware from day 1.
7	SFP Transceivers	All the Transceivers/Modules used to connect the Switches should be from the same OEM/make of the switches only. Switch should support 1Gbps and 10Gbps models.
Hardware Specification		
1	Centralized wire capacity	Switch at least 14 Tbps switching bandwidth or more
2	Per Slot Switching Capacity	3.2 Tbps or more
3	Total number of IPv4 routes	Total number of IPv4 routes 112000 or more,
4	VLANs (802.1q tagged VLAN)	4000 or more Concurrent
5	Memory	8GB D RAM or more
6	Storage	4GB SSD/Flash or more
Support		
1	Switches must be supported for a minimum of 5 years by the hardware vendor with software updates and upgrades without additional cost.	

2	The OEM should provide support services 24x7 TAC with L1, L2 and L3 for 5 years free of cost. India toll free number should be reflected in official website of the OEM.

    ii)   Distribution Switches for Site Locations

   a) Distribution Switch – Type 1

Sl. No.	Description	
1	Form Factor	19 Inch Rack mountable Ethernet
2	Architecture	Non-Blocking architecture. Must have EAL3/NDcPP or above common criteria certification. Should support ITU G.8032 standard.
3	IPV6 Compliance	All Functionalities of Switch shall be IPV4 and IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software.
4	End of sale	OEM End-of-sale declaration shall not have been released for the quoted model at the time of the bid submission.
5	Feature Availability	All the specified features/ parameters/ certifications must be available on the Technical Bid opening date. Features /parameters /certifications proposed to be available in near future / on roadmap shall not be considered. Switch should support VRF,OSPF,VRRP,BGP protocols.
6	Ports	Should support at least 48X1/10Gbps SFP and 4x10/40 ports should be Ready from day 1.
7	SFP Transceivers	All the Transceivers/Modules used to connect the Switches should be from the same OEM/make of the switches only. Switch should support up-to 1Gbps and 10Gbps models
Hardware Specifications:		
1	Back Plane Bandwidth	1.2 Tbps switching bandwidth or more
2	Packet throughput	700 Mpps or more
3	MAC Addresses and MTBF	225K or more and MTBF 585000 Hrs. or more
4	VLANs (802.1q tagged VLAN)	4000 or more Concurrent

5	Memory	2GB DDR or more,
6	IPV6 host	24K
7	Storage	4GB Flash/SSD or more
Support		
1	Switches must be supported for a minimum of 5 years by the hardware vendor with software updates and upgrades without additional cost.	
2	The OEM should provide support services 24x7 TAC with L1, L2 and L3 for 5 years free of cost. India toll free number should be reflected in official website of the OEM.	

b) Distribution Switch – Type 2

Sl. No.	Description	
1	Form Factor	19 Inch Rack mountable Ethernet
2	Architecture	Non-Blocking architecture. Must have EAL3 /NDcPP or above common criteria certification. Should support ITU G.8032 standard.
3	IPV6 Compliance	All Functionalities of Switch shall be IPV4 and IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software.
4	End of sale	OEM End-of-sale declaration shall not have been released for the quoted model at the time of the bid submission.
5	Feature Availability	All the specified features/ parameters/ certifications must be available on the Technical Bid opening date. Features /parameters /certifications proposed to be available in near future / on roadmap shall not be considered. Switch should support VRF,OSPF,VRRP,BGP protocols.
6	Ports	Should Support at least 24x1/10Gbps SFP+ and 2x10/40/100 Gbps ports should be ready from day 1
7	SFP Transceivers	All the Transceivers/Modules used to connect the Switches should be from the same OEM/make of the switches only. Switch should support up-to 1Gbps and 10Gbps models
Hardware Specifications:		

1	Back Plane Bandwidth	800 Gbps switching bandwidth or more
2	Packet throughput	600 Mpps or more
3	MAC Addresses and MTBF	225K or more and MTBF 415000 Hrs. or more
4	VLANs (802.1q tagged VLAN)	4000 or more Concurrent
5	Memory	2GB DDR or more,
6	IPV6 host	24K
7	Storage	4GB Flash/SSD or more
Support		
1	Switches must be supported for a minimum of 5 years by the hardware vendor with software updates and upgrades without additional cost.	
2	The OEM should provide support services 24x7 TAC with L1, L2 and L3 for 5 years free of cost. India toll free number should be reflected in official website of the OEM.	

iii)   Access Switches for Site Locations

a) *Access Switch – Type 1*

Sl. No.	Description	
1	Form Factor	19 Inch Rack mountable Ethernet switch with 1RU form
2	Architecture	Non-Blocking architecture. Must have EAL3 /NDcPP or above common criteria certification. Should support ITU G.8032 standard.
3	IPV6 Compliance	All Functionalities of Switch shall be IPV4 and IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software.
4	End of sale	OEM End-of-sale declaration shall not have been released for the quoted model at the time of the bid submission.
5	Feature Availability	All the specified features/ parameters/ certifications must be available on the Technical Bid opening date. Features /parameters /certifications proposed to be available in near future / on roadmap shall not be

		considered. Switch should support SNMP V2c and V3, 802.1AB, 802.1BA API and SDN-OpenFlow or equivalent feature, PBR or equivalent
6	Ports	24-port Access Switch: Minimum of 24 ports 10/100/1000 Base T, POE/POE+ and 2 x10G SM SFP ports, 1 x Out of Band IP based management Port, 1 Console Port, 0°C to 45°C operating temperature, and, 10% to 90% relative humidity. Should have 16 K MAC Address, 2000 active VLANs.
7	Basic Layer-3 Support	Switches must be managed Basic Layer-3 type for better broadcast segmentation.
8	SFP Transceivers	All the Transceivers/Modules used to connect the Switches should be from the same OEM/make of the switches only.
Hardware Specification		
1	Back Plane Bandwidth	At-least 128 Gbps switching bandwidth
2	Packet throughput	95 Mpps or more for each member switch
3	MAC Addresses and MTBF	MAC - 16K or more and MTBF 300000 Hrs. or more
4	VLANs (802.1q tagged VLAN)	4000 or more Concurrent
Support		
1	Switches must be supported for a minimum of 5 years by the hardware vendor with software updates and upgrades without additional cost.	
2	The OEM should provide support services 24x7 TAC with L1, L2 and L3 for 5 years free of cost. India toll free number should be reflected in official website of the OEM.	

b) *Access Switch (Industrial Grade) – Type 2*

SI. No.	Description	
1	Back Plane Bandwidth	At-least 24 Gbps switching bandwidth or more
2	Packet throughput	16 Mpps or more
3	Type	Manageable Industrial Grade Switch. Should support ITU G.8032 standard.

4	Ports	Minimum 8 x of 10/100/1000 RJ45 and 4 x 1G SFP interface. Simultaneous active port count should be 10 or more.
5	Performance and Reliability	It should be industrial grade switch. Should support operate at wider temperature range (-20 to 70 degree C) withstands greater shock, vibrations, temperature and EMI/EMC tests. MTBF value not less than 200000 Hrs. NEMA Compliant
6	Power	46-58 V DC Redundant power input; POE Budget – 240 watts; Simultaneous 802.3at PoE+ for min 8 ports. Support for IEEE 802.3af as well.
7	VLAN support	a. Minimum 1000 active VLANS b. Dynamic VLAN with VTP / MVRP c. IP subnet Vlan
8	Security	a. 802.1x support b. MAC-based Authentication c. DHCP relay ipv4/ipv6, Snooping d. ACL based on L2, L3, L4 rules e. IP source Guard
9	Surveillance Traffic handling Features:	a. 8K MAC table b. 8 QOS queues per port, DSCP remarking c. NTP over IPv4/IPv6
10	Certification	IEC, ROHS and safety certification
11	Operating conditions	temperature -20 ~ 70°C, humidity 5% to 90% (Non-condensing)
12	Accessories & OEM Criteria	1) The OEM should provide support services 24x7 TAC with L1, L2 and L3 for 5 years free of cost. India toll free number should be reflected in official website of the OEM. 2) For campus solution (other than DC/DR) Core switches, Distribution switches, Access switches and Fiber modules should be from the same OEM.
Support		
1	Switches must be supported for a minimum of 5 years by the hardware vendor with software updates and upgrades without additional cost.	

iv)   Access Point (Indoor)

Sl. No.	Description
1	Access Points proposed must include tri radios (2.4 GHz, 5 GHz and dedicated sensor WIPS) or Access Points proposed must include dual radios with MU-MIMO and access point for dedicated dual band sensor (WIPS)
2	The access point should be light weight and should support installations above drop ceiling, under ceiling or on wall
3	LED should be available for activity indication
4	Must have 2x IEEE 802.3 Gigabit Ethernet autosensing
5	The access point must have integrated antenna
802.11 ac Features	
6	Must support 4x4 multiple-input multiple-output (MIMO) with Radio 1: 2.4GHz: 3x3 with 3SS or better and Radio 2: 5GHz: 4x4 with 4SS (4X4 -MU-MIMO)
7	Should have dual Radios and should support 256 QAM
8	Should support 1.733 Gbps data rates on dual concurrent radio operations
9	Should support 20, 40 and 80 MHz Channels
10	Should support Maximal Ratio Combining, should support 802.11ac transmit beamforming
Radio Features	
11	Maximum conducted transmit power shall be 23 dBm or more on both 2.4 and 5 GHz
Networking Features	
12	Access points or solution should provide automatic redundancy In-case a site controller fails
13	Must have a dynamic or smart RF management features which allows WLAN to automatically and intelligently adapt to changes in the RF environment
Roaming Features	
14	Along with a controller the Access Points should support fast roaming feature
Security Features	
15	The access point should provide wireless IPS sensor support on both radios
16	The WLAN Solution should support IP filtering.
17	WLAN Solution must support Application Visibility Control (Deep Packet Inspection) at both Controller.
18	WLAN Solution must support personal and enterprise WPA2 authentication for a staff WLAN concurrent with open access public WLAN

19	Security solution must provide Rogue AP detection by comparing the MAC address forwarding tables in common enterprise class Ethernet LAN switches
20	Security solution must provide air termination of Rogue Aps
Management Features	
21	WLAN solution should provide features that provides no touch AP discovery, adoption, provisioning
22	WLAN solution should provide features that provides other management functions including firmware push and statistics
23	Must support telnet and/ or SSH login to Aps directly for troubleshooting flexibility
Power	
24	Access point should have Integrated PoE and power injector Support
QoS Support	
25	The Access Points should support WMM, WMM-UAPSD, 802.1p, Diffserv and TOS
26	Support for Voice-over-wireless LAN (VoWLAN) quality of service (QoS) ensures toll quality, even with many simultaneous calls on a single access point
Certification	
27	Access points must have WiFi Alliance certification for 802.11n and 802.11ac
Support	
28	Access point must be supported for a minimum of 5 years by the hardware vendor with software updates and upgrades without additional cost.

v)   Wireless Controller for Access Points

SI. No.	Description
1	WLC should support 1+1 failover for high availability.
2	The proposed WLC must be compliant with IEEE CAPWAP or equivalent for controller-based WLANs.
3	The proposed WLC should be 1U, rack-mountable appliance with 2 x 1G (or better) Ethernet interface. USB support and RS-232 serial console (RJ-45) interface.
4	The proposed WLC should support both centralized as well as distributed traffic forwarding architecture from day 1. It should be IPv6 ready from day one.

5	The proposed controller should support minimum 16K users/devices and WLANs-256.
6	The proposed WLAN controller should be supplied with minimum 100 AP license from Day-1 and can scale up to 500 APs without change / additional hardware. Additional AP license will be procured in future.
7	The wireless access points must securely download image from WLC and should be configured from WLC only.
8	The proposed WLC should support L2/L3 roaming for mobile clients
9	The proposed WLC should provide real-time radio power adjustments based on changing environmental conditions and signal coverage adjustments. It should also adjust radio channel automatically.
10	Should support dynamic bandwidth selection among 20Mhz, 40 MHz, 80Mhz and 160 MHz channels.
11	Controller should support Wi-Fi 6, 802.11ax technology
12	The proposed system must support coverage hole detection and correction that can be adjusted on a per WLAN basis.
13	Should support web-based authentication to provide a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant.
14	Should support port-based and SSID-based IEEE 802.1X authentication.
15	Should support MAC authentication to provide simple authentication based on a user's MAC address.
15	Should support AP grouping to enable administrator to easily apply AP-based or radio-based configurations to all the APs in the same group
16	Plug-and-Play Fast and easy zero-touch installation plus rule-based access point adoption from all locations automates equipment discovery and deployment.
17	WLC should support Comprehensive Integrated Network Security Services Wired/wireless, built-in Wireless Intrusion Protection System (WIPS), and secure guest access with Captive web portal or equivalent solution.
18	WLC should provide BYOD Support. It should provide device fingerprinting and required to help manage and secure user-owned devices.
19	WLC should support 802.11w to secure management frames, NAC integration support
20	WLC should support guest access with Analytics/reporting.
21	WLC architecture should support tunnel forwarding and local forwarding

SI. No.	Description
22	WLAN Solution should support captive portal with time-based access, Customize Guest page and must have option for self-guest registration options, so that guest can automatic register himself from day 1 or with equivalent solution.
23	System/Solution should provide safeguard from DOS attacks and Intrusion Detection and termination of Rogue Access Points.
24	System/Solution should support detection of Impersonation attack, Decryption failures, Invalid MAC transmission, Fake AP attack, Invalid 802.1x frames, Invalid source and destination address
25	WLAN Solution should have feature to create captive portal guest users for authenticating using their User ID (Email Address/ Mobile Number/ Member ID) and the received pass code on Email or SMS in order to complete the registration process.

vi)   Network Access Control Specification

SI. No.	Description
1	Dedicated redundant hardware Appliance or virtualized platform and one Centralized Console. Should be supplied with 1000 AAA (Endpoint Security) licenses.
2	Should be able to integrate with all makes of manageable network devices which can support open standard based protocols required for NAC operation
3	Must provide Network Access Control, End point Integrity Check and visibility in single pane of glass for the entire infrastructure from day 1 spread across multiple Network Locations / Zones
4	Each appliance should scale to at least 10000 devices
5	Solution must utilize standards-based authentication mechanisms enabling non-intelligent devices the ability to connect to the network and receive the proper network services.
6	Should be able to gather Detailed identity and access information with OS and device fingerprinting for Blackberry, Symbian, iOS, Android, OSX, Windows and more
7	Should be able to perform posture check for compute end points (Windows & MAC) for OS health for parameters like Registry Keys, allowed process, AV or Firewall Enabled etc.
8	Detect and protect any device with IP address without the need for a client application on each endpoint including detection of VoIP phones, printers, wireless devices, machinery, cameras, sensors etc.

9	Should be able to perform VAPT check using custom built-in scanner for network-based vulnerabilities
10	Able to build Interactive topology maps to locate the end systems per network connectivity
11	Device search functionality by attributes such as user name / OS type / IP- MAC address / System Name
12	Must Support location-based Registration portals to redirect Users entering through common location to different portals for different Network Zones
13	Must support automated context-based policy provisioning of network services for mobile devices
14	Must provide interoperability with Microsoft NAP and Trusted Computing Croup TNC.
15	Support Management Access Authentication and Authorization for Network Device Access
16	Support Manipulation of Radius Attributes for Authentication as well as Radius Accept
17	Must have SNMP MIB compile capability to integrate any 3rd party snmp compliant device
18	Must be able to create correlated topology based on LLDP, SNMP, L2 and L3 protocol connectivity hierarchy
19	Must provide the capabilities to modify, filter, and create your own flexible views of the network devices based on selectable SNMP OID
20	Must allow scheduled events or tasks that the user can perform behind the scenes or schedule an event for another time in the future.
21	Must provide a utility to view and select MIB objects from a tree-based representation
22	Must provide a Country wide VLAN monitoring capabilities.
23	Must provide comprehensive remote management support for all proposed network devices as well as any SNMP MIB-I or MIB-II manageable devices.
24	Must support RADIUS or LDAP Authentication for users of the application.
25	Must provide a tool to search and locate the physical location of connected devices and end users, quickly and easily.
26	Must allow IT administrators to easily define number of pre-configured network policies, and designate select personnel to activate/deactivate these policies as appropriate
27	Must support the ability to present detailed configuration information including date and time of configuration saves, firmware version, and file size.

vii)   OEM Element Management System (EMS) Specification

SI. No.	Description
1	NMS should be from the same OEM providing switching and wireless solution
2	It Should have Single Pane of Glass Overview of the network
3	NMS Solution should be virtual / hardware-based appliance
4	Must be able to support minimum 100 Switches and should be scalable to support minimum 1000 switches on the same virtual appliance
5	Must be able to create correlated topology based on LLDP, SNMP, STP connectivity hierarchy
6	Must provide centralized management that should be able to manage wired, wireless & security components of 3rd party OEMS's
7	Must allow system-level operations such as device discovery, event management, logging and application maintenance to be performed centrally.
8	Must provide the capabilities to modify, filter, and create your own flexible views of the network.
9	Must allow for graphing or viewing in table format and multiple OIDs that are user selectable.
10	Must allow scheduled events or tasks that the user can perform behind the scenes or schedule an event for another time in the future.
11	Must provide a utility to view and select MIB objects from a tree-based representation and include a compiler for new or third-party MIBs.
12	Must provide a system wide deployment of VLAN configuration and monitoring capabilities.
13	Must provide comprehensive remote management support for all proposed network devices as well as any SNMP MIB-I or MIB-II manageable devices.
14	Must support RADIUS and LDAP Authentication for users of the application.
15	Must have SNMP MIB compile capability to integrate any snmp compliant device
16	Must be able to define policies to rate-limit bandwidth, throttle the rate of new network connections, prioritize based on Layer 2 or Layer 3 QoS mechanisms, apply packet tags, isolate/quarantine a particular port or VLAN, and/or trigger pre-defined actions.
17	Must provide a tool to find the physical location of systems and end users, and where they are connected, quickly and easily.
18	Must provide automated functionality to ensure that appropriate services are available to each user, no matter where they log on.

19	Must support features to interact with 3rd party network security devices to provide automated response to security events and thus remediating real time threats
20	Must provide an audit trail (event log).
21	Must be able to integrate with NAC and Wireless devices
22	Must allow IT administrators to easily define a number of pre-configured network policies, and designate select personnel to activate/deactivate these policies as appropriate
23	When integrated with compatible WLAN it must be able to provide granular management functionalities like system location and tracking, wi-fi dashboards, client search, event logs etc via mobile devices as well such as tablet and smartphone
24	Must provide a detailed inventory of products organized by device type.
25	Must provide the ability to track device attributes such as serial number, asset tag, firmware version, CPU type and memory.
26	Must support he ability to present detailed configuration information including date and time of configuration saves, firmware version and file size.
27	Must record a history of device attributes and reports any changes made to the device.
28	Must be able to provide a history of firmware and configuration changes made to the device.
29	Must be able to generate valuable, in-depth reports for network inventory for planning purposes.
30	Must provide a centralized history of inventory management operations.
31	Must support the liability to download firmware to single or multiple devices simultaneously.
32	Must be able schedule route device configuration back-ups.
33	Must be able to download text-based (ASCII format) configuration templates to one or more devices.
34	Must instantly identify the physical location and user profile where an attack was sourced.
35	Must be able to take action based on a predefined security policy, including the ability to notify the intrusion detection system of the action taken via a SNMPv3 trap (inform).
36	When integrated with security devices such as NAC or IDS it must be able to isolate and quarantine the attacker without disruption to other users, applications and business critical systems.

37	When integrated with security devices such as NAC or IDS it must be able to dynamically deny, limit or change the characteristics of the user's access to the network.
38	Must provide a web interface that contains reporting, dashboards, troubleshooting and monitoring tools.
39	Must provide web-based flexible view, device views and event logs for the entire infrastructure.
40	Must enable diagnosis of network issues and performance through real-time NetFlow analysis.
41	Must provide port level analysis capability.
42	Must provide customizable reports.
43	Must be able to write Python scripts to integrate with IoT solutions.
44	Should have the capability to integrate with 3rd Party Vendors.
45	Should have the capability to reduce risk and ensure your network configurations comply to HIPAA and PCI with that analyses and assesses network configuration for compliance across your entire wired and wireless network.
46	Should have the ability to get actionable business insights and speeding up troubleshooting by separating network from application performance so you can quickly identify root-causes, monitors shadow IT, reports malicious or unwanted applications and assesses security compliance.

2.5.   WiFi

i)   Access Point (Outdoor)

SI. No.	Description
Accepted Make: Cambium, Ruckus, Cisco, Aruba, Radwin	
1	Access Points proposed must include dual radios (2.4 GHz and 5 GHz) and should cover a distance of 2 kms in open area
2	The access point should be light weight and should support installations on walls or light poles without disturbing the aesthetics of the area.
3	LED should be available for activity indication
4	Must have 2x IEEE 802.3 Gigabit Ethernet autosensing
5	The access point must have integrated antenna
802.11 ac Features	

6	Must support 2x2 multiple-input multiple-output (MIMO) with Radio 1: 2.4GHz: 2x2 with 2SS or better and Radio 2: 5GHz: 2x2 with 2SS
7	Should have dual Radios and should support 255 clients
8	Should support 1.3 Gbps data rates on dual concurrent radio operations
9	Should support 20, 40 and 80 MHz Channels
10	Should support Maximal Ratio Combining, should support 802.11ac transmit beamforming
Radio Features	
11	Maximum conducted transmit power shall support 23 dBm or more on both 2.4 and 5 GHz
12	The antenna gain should be 4 dBi or more
Networking Features	
13	The access point or the controller should support DHCP relay
14	Must have a dynamic or smart RF management features which allows WLAN to automatically and intelligently adapt to changes in the RF environment
15	WLAN Solution should support Mesh capabilities
Roaming Features	
16	Along with a controller the Access Points should support fast roaming feature
17	**Security Features**
18	The access point should provide wireless IPS sensor support on both radios
19	The WLAN Solution should support IP filtering
20	WLAN Solution must support Application Visibility Control (Deep Packet Inspection)
21	WLAN Solution must support personal and enterprise WPA2 authentication for a staff WLAN concurrent with open access public WLAN
22	Security solution must provide Rogue AP detection by comparing the MAC address forwarding tables in common enterprise class Ethernet LAN switches
Management Features	
23	WLAN solution should provide features that provides no touch AP discovery, adoption, provisioning
24	WLAN solution should provide features that provides other management functions including firmware push and statistics

25	Must support telnet and/ or SSH login to Aps directly for troubleshooting flexibility
Power	
26	Access point should have Integrated PoE and power injector Support
QoS Support	
27	The Access Points should support WMM, WMM-UAPSD, 802.1p, Diffserv and TOS
28	Support for Voice-over-wireless LAN (VoWLAN), quality of service (QoS).
Certification	
29	Access points must have WiFi Alliance certification for 802.11n and 802.11ac
30	Access points must have WiFi Alliance certification for WPA2 Enterprise
Support	
31	Access point must be supported for a minimum of 5 years by the hardware vendor with software updates and upgrades without additional cost.

2.6. Campus Backbone Cabling

i) Fiber Termination Box

Sl. No.	Description
1	Data Sheets in support of below to be provided
2	19-inch rack mounted,
	Upto 2U height for 48-Fiber panels; 1U height for 24 fiber panels
3	Couplers: Panel fully loaded with Duplex LC SM Couplers and pigtails
	zirconia-ceramic sleeves, rated for minimum of 220 cycles mate & un-mate; integrated dust / protective caps preferred
4	Built-in Fusion Splice tray – 48 Fibers
5	Minimum 4 numbers of rubber cable glands in rear for entry of 15mm cables
6	Integrated fiber management
7	1.2mm/ 16 gauge steel, powder coated, drawer style to facilitate on-site splicing
8	Adequate provision for label holders and labelling

ii) Optical Fiber Cable (OFC)

Sl. No.	Description
1	Data Sheets in support of below to be provided
2	Construction:
	Outdoor armoured cable – suitable for direct burial as well as ducted applications;
	Loose Tube, corrugated Steel Armoured Cable;
	UV resistant jacket;
	Multi-loose tube, moisture blocking gel-filled, Dielectric central element reinforcing, surrounding by water blocking tape and aramid yarns;
	cable weight less than 180Kg/KM;
	cable diameter less than or equal to 15mm;
	12-core and 6-core types
3	Fiber Type: ITU-T G.652.D, 250 micron buffered
4	Maximum core / clad offset: 0.5 microns
5	Tensile load 800N maximum, vertical rise 500m maximum
6	Operating temperature: -20 Degrees C to +70 Degrees C
7	RoHS compliant
8	Attenuation: 0.5dB/KM or better @ 1310nm and 1550nm or better

iii) Optical Fiber Pigtails

Sl. No.	Description
1	Data Sheets in support of below to be provided
2	LC Simplex pigtails, 1m length
3	SM, 2mm buffered jacketed Fiber, RoHS compliant
4	Insertion Loss: less than 0.3dB
5	Return Loss: greater than 45dB
6	End-face: OEM should certify compliance to IEC 61300-3

iv) Optical Fiber Cable (OFC) Patch Cord

Sl. No.	Description
1	Data Sheets in support of below to be provided
2	LC-LC Duplex patch cords,
3	Assorted lengths: 3m, 5m,

SI. No.	Description
4	SM, 2mm zip-cord, RoHS compliant
5	Insertion Loss: less than 0.3dB
6	Return Loss: greater than 45dB
7	End-face: OEM should certify compliance to IEC 61300-3

v) CAT 6A Cable

SI. No.	Description
1	The Copper Cabling system shall be made up of 4-pair, Cat6A U/UTP LSZH cabling system.
2	The proposed U/UTP cabling system shall comply with 4-connector channel as well as permanent link performance specifications of the latest revisions of the TIA 568 (or equivalent ISO/ IEC 11801) standard. Documented data sheets shall be furnished by MSP / OEM.
3	All end points of the network will connect to the Passive Network Infrastructure using Cat6A U/UTP Cabling System.
4	All components of the U/UTP Cabling system proposed by a MSP should be from a single OEM.
5	It is preferable to have all components of the proposed U/UTP cabling system from an OEM be from a single, documented, publicly published, cabling solution set.
6	Cat6A U/UTP cabling system shall support 1000BASE-T Ethernet, 2.5GBASE-T and 5GBASE-T Ethernet, 10GBASE-T, as well as, Type 1, Type 2, Type 3, and Type 4 PoE delivery over a full 100m 4-connector channel. MSP to furnish documented proof for support of such applications.
7	The proposed Cat6A U/UTP cabling system shall comply performance of the following performance parameters for a 100m 4-connector Channel with the requirements of the latest revisions of TIA 568 standard
	DC Resistance and DC Resistance Unbalance; Insertion, NEXT, PSNEXT and Return Losses; ACRF and PSACRF; TCL and ELTCTL; Propagation Delay and Propagation Delay Skew; PSANEXT and PSAACRF
8	MSP shall submit OEM documentation supporting performance compliance of proposed Ca6A U/UTP cabling systems to the channel specifications to the latest revision of TIA 568 standard. Such documentation should include the manufacturers part numbers that make up the 4-connector channel.
9	Performance headroom (worst case margins only), if any guaranteed by the OEM, for parameters specified above may be included in the OEM's

Sl. No.	Description
	supporting documentation for channel specification. If is preferred that such documentation be a publicly published one.
10	Third party test reports of compliance of the performance parameters to the channel specifications of TIA 568 standards clearly indicating the part numbers that comprised the testing shall be included if available.
11	OEM certification for providing a 25-year performance warranty (upon installation and acceptance testing) shall be included for guaranteeing
	Performance compliance to channel performance specifications.
	Performance (successful delivery) of applications as listed above.
	Data sheets should be provided in support of above specification by MSP/ OEM
12	Manufacturers: CommScope Netconnect, Belden, Panduit etc.
13	Data sheet(s) in support of below to be provided.
14	Should meet channel specifications of latest TIA 568 standard for Cat6A when used as a component in the installed Cat6A U/UTP channel.
15	23 AWG, U/UTP cable, 4-pair, CMR
16	Breaking strength: 400N (maximum)
17	Electrical Performance as per latest revision TIA 568 (or equivalent ISO/IEC standards) to Cat6A U/UTP performance requirements respectively
	DC Resistance and DC Resistance Unbalance
	Insertion, Return, NEXT, PSNEXT losses
	ACRF and PSACRF
	TCL and ELTCTL
	Propagation Delay and Propagation Delay Skew
	PSANEXT and PSAACRF
18	UL approved
19	Fire rating: IEC 60332
20	RoHS compliant
21	Any 3rd party test reports for electrical, mechanical and fire-rating performance to be included

vi) CAT 6A Patch Cord (2 Meter)

Sl. No.	Description
1	Data Sheets in support of below to be provided
2	Should meet channel specifications of latest TIA 568 standard for Cat6A when used as a component in the installed Cat6 U/UTP channel

3	100 ohms, Solid copper, 24AWG
4	CM jacket, with plug boot
5	Insertion life: 750 mate & un-mate cycles
6	Any 3rd party test reports for electrical, mechanical and fire-rating performance to be included

     vii)   CAT6A UTP Information Outlet

SI. No.	Description
1	Data Sheets in support of below to be provided
2	Should meet channel specifications of latest TIA 568 standard for Cat6A when used as a component in the installed Cat6 U/UTP channel.
3	8-position, 4-pair, UTP jack, with IDC contacts supporting 22 AWG to 24 AWG solid conductors.
4	Electrical Performance as per latest revision TIA 568 (or equivalent ISO/IEC standards) to Cat6A U/UTP performance requirements respectively
	DC Resistance and DC Resistance Unbalance; Insertion, Return, NEXT and PSNEXT losses; FEXT and PSFEXT losses; TCL and TCTL; Propagation Delay and Propagation Delay Skew; PSANEXT and PSAFEXT losses
5	**Durability:**
	Min 750 mate & un-mate cycles for plug interface; Min 20 re-terminations for the IDC punch down contacts
6	**PoE Support:** Support Type 1, Type 2, Type 3 and Type 4 PoE levels
7	**Operating temperature**: -10 Degree C to +60 Degrees C
8	UL approved.
9	RoHS Compliant

     viii)   CAT6A Jack Panel

SI. No.	Description
1	Data Sheets in support of below to be provided
2	Should meet channel specifications of latest TIA 568 standard for Cat6A when used as a component in the installed Cat6 U/UTP channel.
3	19", 1U, straight, 24-port, un-loaded (support discrete modular jacks), metal frame, with integrated label holder
4	Rear Cable bar should be included in supplies

Sl. No.	
5	Modular Jack of the panel should meet the specifications of Modular Jacks for electrical, durability, PoE support and operating temperature specified above
6	UL approved, RoHS compliant

ix)　CAT6A U/UTP MPTL Plugs

Sl. No.	Description
1	Data Sheets in support of below to be provided
2	Should meet channel specifications of latest TIA 568 standard for Cat6A when used as a component in the installed Cat6 U/UTP channel.
3	Cable side termination: 8-position, 4-pair, UTP jack, with IDC contacts supporting 22 AWG to 24 AWG solid conductors, 20 re-terminations durability
4	Plug/Jack compatibility: RJ45 style, 750 mate & un-mate cycles durability
5	Electrical performance, PoE support, operating temperature specifications same as that for modular plug
6	UL approved and RoHS compliant

x)　CAT 6 Cable

Sl. No.	Technical Specifications
1	This cable well exceeds the requirements of TIA/EIA-568-C.2 and ISO/IEC 11801
2	Construction: 4 twisted pairs separated by internal X shaped, 4 channel, polymer spine / full separator. Half shall not be accepted.
3	The 4 pair Unshielded Twisted Pair cable shall be UL☐ Listed. Cable should also be tested and verified by ERTL.
4	Conductor Solid Bare Copper and Jacket FR PVC and UL approved CM rated cable and Outer jacket sheath of the cable shall be LSZH.
5	Insulation: High Density Polyethylene
6	Dielectric Strength of cable should be 1.0KV dc
7	Attenuation (< 17 db), Pair – to – pair and PS NEXT, ELFEXT and PSELFEXT, Return Loss, ACR and PS ACR.
8	Bending Radius should be < 25.4mm at –20°C ± 1°C and Pulling Force: 11.5 Kg
9	Nominal Outer Diameter of Cable should be 6.1 mm and Conductor Diameter 0.56 mm (23 AWG)
10	Cable should support operating Temperature from -20° to +70°C

11	Cable should come with printed sequential Length Counter on each meter
12	Cable support Conductor Resistance < 9.38 Ω /100m
13	Mutual Capacitance of cable should be < 5.6nF/100m
14	Max Resistance Unbalance of cable should be 5% Max
15	Capacitance Unbalance of cable should max 330pF/100m
16	Cable support Delay Skew: < 45nS, Operating Voltage: 72V and NVP: 69%
17	Category 6 UTP cables shall Supports Gigabit Ethernet (1000 base-T) standard and Operates at bandwidth of 600MHz.

xi)   CAT6 Patch Cord (2 Meter)

Sl. No.	Description
1	Equipped with modular 8-position modular plugs on both ends, wired straight through with standards compliant wiring.
2	The Patch cords shall, at a minimum comply with proposed ANSI/TIA/EIA-568-C.2 Commercial Building Cabling Standards Transmission Performance Specifications for 4 pair 100☐ Category 6 Cabling.
3	Should have 50 micro inches of gold plating over nickel contacts.
4	Should be covered by ETL verification program for compliance with TIA 568.C.2
5	Conductor size: 24 AWG stranded bare copper
6	Cable flame property should follow VW-1 and FT-1 Standard
7	Jacket: PVC UL-94V-O
8	Temperature range: -10oC to +80oC
9	Operating life: Minimum 750 insertion cycles
10	Contact blade: Phosphor bronze
11	Contact plating: 50µ" Gold
12	Plug dimensions & tolerances compliant with FCC Part 68.500 and IEC 60603-7
13	UL approved for copper conductor
14	Dielectric withstanding voltage: 150 V AC
15	Insulation resistance: 35 M Ohm (Max)
16	Cable length: 2 Meter

xii)   CAT6 UTP Information Outlet

Sl. No.	Description

1	INFORMATION OUTLET should support Category 6, ANSI/EIA/TIA568 C.2 and 568A/B configuration
2	All information outlets for 100 ⯀, 22-26 AWG copper cable shall: Use insulation displacement connectors (IDC)
3	Allow for a minimum of 200 re-terminations without signal degradation below standards compliance limits.
4	Be constructed of high impact, flame-retardant thermoplastic with color and icon options for better visual identification.
5	IDC Contact Plating: Phosphor bronze with tin plated and Housing PC + glass fiber (UL 94 V-2)
6	Insertion force: 20N max (IEC 60603-7-4)
7	Contact Plating: 50 μ inches gold on plug contact area
8	Information outlet (RJ45 jack) should be covered under ETL Verification program for compliance with TIA 568.C.2
9	Operation Temp: -10 C to 60 C
10	Plastic Housing: Polycarbonate, UL94V-0 rated or equivalent
11	Operating Life: Minimum 750 insertion cycles
12	Contact Material: Copper alloy
13	Surface mount box with single RJ45 socket to terminate UTP CAT 6 Cable

xiii)   CAT6 Jack Panel

Sl. No.	Technical Specifications
1	The Cat-6 transmission performance is in compliance with ANSI/TIA-568-C.2, ISO/IEC 11801 Ed.2 and EN 50173-1 specification with LED indicator at each Port.
2	Allow for a minimum of 200 re-terminations without signal degradation below standards compliance limit and Fast-Location lighting cable identification technology for saving cost and time for cable identification
3	Have port identification numbers on the front of the panel with writable and erasable marking surfaces for each port on the front panel.
4	Should have self-adhesive, clear label holders and white labels with the panel should be of 1U height with 24 port un-loaded IO.
5	IDC: Suitable for 22-26 AWG stranded and solid wire compatible with both 110 & Krone punch down tools.
6	Each port / jack on the panel should be individually removable on field from the panel.
7	IDC cap: ABS, UL 94V -2 and Phosphor bronze with tin plated and Made of powder coated steel

8	Plastic Housing: Polycarbonate, UL94V-0 rated or equivalent
9	Dielectric Strength: 1000V RMS for 1min
10	IDC Operating life: minimum 250 insertions and Jack Operating life: minimum 750 insertions
11	Insulation Resistance: 10M Ω min, Contact Resistance: 2mΩ per contact
12	Temperature Range: -10℃ to 60℃ max, Humidity :10%-65%
13	PCB: FR-4,1.6mm thickness, Panel : SECC,1.5mm thickness
14	Plug Retention Force: 15 lb and Jack Contact: phosphor bronze,50μ Inch thickness gold over nickel
15	IDC Contact: 0.8mm thickness phosphor bronze, tin plating over nickel
16	Should be rack mountable

xiv)　　CAT6/6A Faceplates

Sl. No.	Description
1	Data Sheets in support of below to be provided
2	Fire -retardant Plastic, ABS,
3	1-port and 2-port styles, each port with spring Shutters
4	British Style, Square, white color
5	UL approved and RoHS compliant
6	Support Modular Jacks specified above
7	Integrated label holder
8	Back-box to be separately supplied for surface mount applications

xv)　　Surface Mount Box

Sl. No.	Description
1	Data Sheets in support of below to be provided
2	Fire -retardant Plastic, ABS,
3	1-port, 2-port and 12-port styles, white color
4	UL approved and RoHS compliant
5	Support Modular Jacks specified above

xvi)   Network Rack

Sl. No.	Description
42U Rack	
1	Racks should be 7' high with dimensions of 800mm x 1000mm suitable for mounting equipment and panels for network applications
2	Racks should provide sufficient cable entry and exit cut-outs in top and bottom of the rack
3	Integrated fan module – 4 fans with tray
4	Rack should support static load of at least 750 KGs on Casters and Levellers.
5	Racks should have a tough glass front door and steel sheet, split rear door.
6	Front and back doors shall have door handles and provided with locks.
7	For offering greater mounting flexibility of equipment, the rack should have 4No's adjustable, 19" verticals with punched 10mm square hole and Universal 12.7mm-15.875mm-15.875mm alternating hole pattern.
8	Rack should have numbered U positions to easily locate positions for mounting as well as identifying equipment.
9	All mounting hardware should come along with the rack
10	Side panels to be included. Side panels should sit flush with the rack and do not take up additional space
11	Rack should be supplied along with 4 Nos. of 1U covered horizontal Cable managers
12	Rack should be supplied along with 2 Nos. of covered vertical Cable managers
13	Rack should have provision for grounding and bonding. All accessories for grounding and bonding shall be supplied along with tacks.
14	1 number of tray/ shelve
15	All sheet metal parts should be Pre-Treated and powder coated meeting ASTM Standard.
16	Racks shall be UL listed and RoHS compliant
17	Supply with 2 numbers of Vertical PDUs, Rack PDU SNMP enabled for Core Switches / Non-SNMP enabled for Distribution Switches, metered by Outlet with Switching, Zero U, 32A, 230V, (21) C13 & (3) C19 (or equivalent) along with all mounting accessories
18	Manufacturers: Rittal, APW, APC, Netrack, Valrack/ Legrand
24U Rack (IP and Non-IP Rated)	

1	Racks should be 24U high with dimensions of 600mm x 800mm suitable for mounting equipment and panels for network applications
2	IP55 rated or above
3	Racks should provide sufficient cable entry and exit cut-outs in top and bottom of the rack
4	Integrated fan module preferred
5	Rack should support static load of at least 750 KGs on Casters and Levellers
6	Racks should have a tough glass front door and steel sheet, split rear door.
7	Front and back doors shall have door handles and provided with locks.
8	For offering greater mounting flexibility of equipment, the rack should have 4No's adjustable, 19" verticals with punched 10mm square hole and Universal 12.7mm-15.875mm-15.875mm alternating hole pattern or equivalent.
9	Rack should have numbered U positions to easily locate positions for mounting as well as identifying equipment.
10	All mounting hardware should come along with the rack
11	Side panels to be included. Side panels should sit flush with the rack and do not take up additional space
12	Racks should be supplied with 2 Nos. of 1U horizontal cable managers.
13	Rack should have provision for grounding and bonding. All accessories for grounding and bonding shall be supplied along with tacks.
14	All sheet metal parts should be Pre-Treated, and powder coated meeting ASTM Standard.
15	1 number of tray/ shelve
16	Racks shall be UL listed and RoHS compliant
17	Supply with 1 number of horizontal PDU, 16A along with all mounting accessories
18	Manufacturers: Rittal, APW, APC, Netrack, Valrack/ Legrand

xvii)   Pre-cast Conical Manhole Chamber

Sl. No.	Description	
1	Size:	Height (With Cover) 800 mm.
		Base Dia (Inner) 810 mm.
		Top Opening (Inner) 550 mm.
		Thickness of each ring 60 mm.
2	Material Used:	M 30 Grade Concrete
3	Reinforcement:	

		In the rings: In the top ring 3 nos. of TOR Steel horizontal rings of size 8mm supported by 8mm TOR Steel bars.
		In top Cover: Multiple nos. of TOR Steel bars both ways.
		Single Layer: 8mm TOR Steel bars.
		The Top Cover guarded by GI M S Plate and provided two 12 mm hooks for lifting.
4	Load Bearing:	Suitable for an ultimate load 20 Tons (H.D. Cover Load as per IS: 12592 Specifications).

xviii)   Earthing Pit

SI. No.	Description
1	17mm diameter X 3 meter Steel High Tensile EN-8D Grade Rod with Copper Bonding of minimum 250 microns, Pre-welded Clamp should have provision to connect external cables & strips.
2	Jam plus compound (03 Nos.)
3	Poly plastic earth pit cover
4	The rod should be CPRI tested
5	Conductive Gel (4 Kg). Polyplastic Earth Inspection Pit Cover. Earth pit cover of 10" diameter (EPC10) with load bearing capacity of more than 8 tones Tested from national Test House.
6	Back fill compound (BFC) Certified by National Test House (Govt. of India Lab) as per IEC 62561-7 and ASTM G57-06 for a resistivity of 0.244 ohms-mtr & tested for PH value of more than 9.

xix)   Spike Lightning Arrestor

SI. No.	Description	
1	Spike	5 Prone
2	MOC	Copper
3	Down Pipe Dia	25 mm
4	Down Pipe Length	1500 mm
5	Base Plate Size	90x90x3 mm

xx)   1kVA Online UPS (Accepted Makes: APC, Vertiv/ Emerson, Numeric, Delta Power)

SI. No.	Specifications	Requirement
1	Capacity (in kVA / kW)	1kVA/0.8kW 1-Phase Input / 1-Phase Output

2	**Technology and Capability**	a) True **Online** configuration with **double conversion** UPS & Zero transfer time. b) DSP based control with advanced technology. c) Wide **Input voltage range** from (110 ~ 280VAC) d) Auto **restart & capability** with the **Independent** battery bank operation of the UPS. e) UPS should be designed at **Rated PF of 0.8 i.e. 1kVA/0.8kW** UPS rating. f) **Generator compatibility** with **cold start** and **AC star**t features. g) Automatic bypass to transfer the load on mains due to overload & internal fault. h) ECO mode should be available in the UPS.
3	**Model Name & Number**	
3.1	1kVA /0.9kW	**Make / Model / Part No** to be specified
4	**Input**	
4.1	Input facility -Phases / Wires	Single-Phase / 2-Wire & Gnd (1Phase & Neutral + Ground)
4.2	Input Voltage Range	80-280VAC Range (Full Load) 175~280VAC Range (50 ~ 100% load is required) 80~175VAC
4.3	Nominal Input Frequency	50/60Hz ± 10Hz
4.4	Input Frequency Range	40 to 70 Hz
4.5	Input Power Factor	> 0.99(@ full resistive load)
4.6	Generator Compatibility	Compatibility to genset supply required
4.7	Input Protection	Should be provided at the input of the UPS suitable for the full rated capacity of the UPS.
5	**Output**	
5.1	Nominal Output voltage	208/220/230/240 VAC
5.2	Output Voltage Regulation	± 1% for linear load
5.3	Nominal Output Frequency	50/60 Hz
5.4	Output Frequency Regulation	± 0.1Hz
5.5	Output Frequency Slew Rate	< 1Hz/sec
5.6	Output Wave Form	Pure sine wave
5.7	Output Voltage Distortion (THDu)	< 3% for linear load & < 6% for non-linear load.
5.8	Crest Factor	3:1 On Full Load (Minimum)
5.9	Output Short circuit Protection	Electronic Protection
6	**Transfer Time**	
6.1	Transfer Time (Mode of operation)	Zero ms from Mains mode to Battery Mode Zero ms from Battery Mode to Mains mode

6.2	Transfer Time (Inverter to Bypass / Bypass to Inverter)	< 4ms
6.3	Automatic Bypass switch	UPS should be capable of automatic change over to bypass.
7	**Efficiency (At Nominal Voltage & Resistive Load up to kW rating of UPS)**	
7.1	Overall Efficiency (AC to AC) - Online (Double Conversion)	Upto 86% (at 100% load)
8	**Overload**	
8.1	Inverter Overload capacity	<105% : continuous ; 105% ~ 125%: 1 minutes; 120% ~ 150%: 30 seconds; >150%: 0.5 seconds only
9	**Display Panel (In-build LC Display & LED)**	
9.1	**Measurements** (On LCD)	Input Voltage & Frequency, Bypass, Output Voltage & frequency, Kilowatt, kVA, ECO mode, Battery & Load Level Indicator, Ambient temperature & Event code.
9.2	**Fault Indication** (On LCD)	Charger warning, Fan fault, Temperature out of Range,+/-DC bus High/Low, Inverter Fault, DC-DC fault, abnormal output/Inverter voltage, output short circuit, charger fault, overload shutdown, battery low shutdown.
9.3	**Setable data**	Inverter Voltage, Inverter Frequency, Standby bypass, ECO, Bypass Range, Buzzer, Battery Capacity, Battery String, & Overload alarm
9.4	**Indications** (LED)	Green & Red
10	**Alarms**	
10.1	Audible Alarms	Charger warning, Fan fault, Temperature out of Range, +/-DC bus High/Low, Inverter Fault, DC-DC fault, abnormal output/Inverter voltage, output short circuit, charger fault, overload shutdown, battery low shutdown.
11	**Battery Backup / Battery Bank & Charger**	
11.1	Backup Required	Depends on the capacity of the battery.
11.2	Battery Bank Voltage	24 V DC
11.3	Batteries Type	Sealed Maintenance Free (SMF) - 12V Cells, VRLA/ GEL, AGM
11.4	Battery Makes	Amara Raja / Exide / HBL / Amco / Rocket
11.5	Number of Battery Banks	Single Bank system.
11.6	Minimum Charger Rating (Including internal / external)	The charger should be able to deliver charging current equivalent to 10% of Battery Ah rating offered. (In-case of external chargers, suitable monitoring of the chargers should be provided in the UPS. Also, all external chargers taking AC input must have PFC - Power factor correction)

11.7	Charger type / Charging Method & Charging Voltages	**Constant Voltage Constant Current** Solid state **SMPS** charger
11.8	Charger current	4A extended upto 8A with internal charger (OPTIONAL)
11.9	Battery Housing (Vendor to provide the GA drawings of the offered Battery Rack)	Should be compact and space saving **MS steel open racks** complete with interconnectors
11.10	Battery End Cell Voltage	1.75 V/cell
12	**Interfaces**	
12.1	USB Port should be available **(Mandatory)**	There should be provision for USB port also in the UPS.
12.2	RS232 Port should be available **(Mandatory)**	There should be provision for RS232 port also in the UPS.
12.3	Interface to NMS (Network Management System)	SNMP (IPV6) Card for connecting the UPS to LAN thru Ethernet port & monitoring thru NMS should be available (The cost of SNMP Card / NMS software to be quoted separately)
13	**Restart / Testing Capability**	
13.1	Cold Start	UPS should start up On AC Supply (Mains) without DC Supply (Batteries) On DC Supply (Batteries) without AC Supply (Mains)
13.2	Automatic Restart	UPS should start up automatically on mains resumption after battery low shutdown
13.3	Self Diagnosis	UPS should be capable to carry out self test of Rectifier / Charger /Battery & Inverter module during start-up
14	**Physical**	
14.1	Operating Temperature	0 to 40 deg C
14.2	Storage Temperature	-15 to 50 deg C
14.3	Operating Humidity	20% ～ 95%RH (No Condensing)
14.4	Operating Altitude	0-1000m
14.5	Type of Cooling	Forced Air
14.6	Noise Level	< 40 dbA at 1 meter distance
14.7	Form Factor	Rack mountable
14.8	Packaging Material / Vibration Withstand & Drop Test	Recyclable (No CFC) & 1. Vibration testing as per ISTA -1G Non-operational with Packing
14.9	Standard Package of UPS to include the following minimum accessories	1. UPS 2. Input cable 3. Battery cable 4. USB cable 5. User Manual
15	**Certifications**	

15.1	Manufacturer	ISO 9001, 14001
15.2	Product Safety Certifications **(Mandatory)**	**BIS Certification**
15.3	Product Safety Certifications **(Mandatory)**	**CE Certification**
15.4	Product Safety Certifications **(Mandatory)**	**RoHS Certification**

xxi)   30kVA Online UPS (Accepted Makes: APC, Vertiv/ Emerson, Numeric, Delta Power)

Sl. No.	Specifications	Requirement
1	**Capacity (in kVA / kW)**	**30 kVA/ 30 kW 3-Phase Input / 3-Phase Output**
2	**Technology and Capability**	a) True **Online** configuration with **double conversion** UPS b) **DSP** based technology with reduction in electronic components. c) Fully rated power **(kVA=kW)** for maximum power availability. d) Possibility of enhancing UPS capacity / redundancy by operating UPS in N**+X Parallel Redundant Configuration(PRS).** e) Capability of **Independent or Common** battery bank operation of the UPS when operated in PRS. f) UPS should be designed at **Rated PF of 1 i.e. 30kVA /30kW** UPS rating. g) Dual Input design. h) UPS should have IGBT topology for both PFC (power factor correction) and inverter. i) Should have **Dual Aux power** design.
3	**Model Name & Number**	
3.1	30 kVA / 30 kW	**Make / Model / Part No** to be specified by the vendor
4	**Input**	
4.1	Input facility -Phases / Wires	3-Phase / 4-Wire & Gnd (3Phase & Neutral + Ground)
4.2	Input Voltage Range	230/400V, 240/415V (3Φ4W) Range (Full Load) 173~276 / 300~477VAC Range (Derating to 70% Load) 132~173 / 228~300VAC
4.3	Nominal Input Frequency	50/60Hz **(Auto-Selectable)**
4.4	Input Frequency Range	45 to 65 Hz
4.5	Input Power Factor	> 0.99 (Full Load)
4.6	Current Harmonic Distortion (ITHD)	< 3%

4.7	Generator Compatibility	Compatibility to genset supply required
4.8	Input Protection (Thru In-built 1P MCB)	Should be provided at the input of the UPS suitable for the full rated capacity of the UPS
5	**Output**	
5.1	Nominal Output voltage	220/380V,230/400V,240/415V (3Φ4W)
5.2	Output Voltage Regulation	± 1 %
5.3	Nominal Output Frequency	50/60 Hz
5.4	Output Frequency Regulation	± 0.05Hz
5.5	Output Frequency Slew Rate	＜1Hz/sec
5.6	Output Wave Form	Pure sine wave
5.7	Output Voltage Distortion (THDu)	< 2 % (linear load)
5.8	Crest Factor	3:1
5.9	Output Short circuit Protection	Electronic Protection
6	**Transient Response / Recovery**	
6.1	Transient Response: Dynamic Regulation for 10% to 90% step linear load	±7% or 60ms
6.2	Transient Recovery to steady state condition after 10% to 90% step linear load	< 1 cycle
7	**Transfer Time**	
7.1	Transfer Time (Mode of operation)	Zero ms from Mains mode to Battery Mode Zero ms from Battery Mode to Mains mode
7.2	Transfer Time (Inverter to Bypass / Bypass to Inverter)	<1ms (Synchronized Mode)
7.3	**Automatic & Bi-directional static by-pass (In-built)**	Bypass To Inverter ±10 % (Rated Voltage) Inverter To Bypass ±7 % (Rated Voltage)
7.4	**Maintenance Bypass**	1.UPS should have option for manual maintenance bypass 2. Maintenance bypass cover removal sensing. 3.The maintenance bypass should provide for Hot-swap of the faulty UPS PWB for repairs / service.
8	**Efficiency (At Nominal Voltage & Resistive Load up to kW rating of UPS)**	
8.1	Overall Efficiency (AC to AC) - Online (Double Conversion)	Upto 96%
8.2	Overall Efficiency (AC to AC) - ECO Mode (Bypass feeding the load under normal conditions)	Upto 99%
9	**Overload**	

9.1	Inverter Overload capacity	≤105 %: continuous,106% ~ ≤125%: 10 minutes; 126% ~ ≤150%: 1 minute; >150%: 1 second
10	**Display Panel (In-build LC Display & LED)**	
10.1	**Measurements** (On LCD)	Input: Voltage / Frequency, Bypass: Voltage / Frequency, Output: Voltage / frequency, Battery: Remaining time / Battery Level Indicator, Load**:** Percentage / Load Level Indicator, Battery Voltage Capacity/Status/Test Result, System Date/Time Setting, Current Time, PFC Fuse Open, Battery Temperature Too High, Battery Over Charge, Battery Out of Date, INV Short Circuit, Output Breaker Off, kVA, kW, output current, Battery current.
10.2	**Fault Indication** (On LCD)	Main Input Sequence Fault, Power Module General Fault, Battery Ground Fault, Bypass Static Switch Fault, Parallel Fault, System General Fault, Provide Bypass O/P Even If UPS Fault.
10.3	**Indications** (LED)	Normal-Green/Battery-Orange/Bypass-Green/Fault-Red
11	**Alarms**	
11.1	Audible Alarms	Battery Low beep / DC Fault beep/ UPS Overload beep/ o/p short ckt fault beep/ Shutdown beep
12	**Battery Backup / Battery Bank & Charger**	
12.1	Backup Required	30 minutes
12.2	Battery Bank Voltage	384 V DC or higher
12.3	Battery Bank VAh (Vendor to include battery sizing calculations with tender)	26000 or higher
12.4	Batteries Type	Sealed Maintenance Free (SMF) - 12V Cells
12.5	Battery Makes	Amara Raja / Exide / HBL / Amco / Rocket
12.6	Number of Battery Banks	Maximum Two Banks in parallel
12.7	Minimum Charger Rating (Including internal / external)	The charger should be able to deliver charging current equivalent to 10% of Battery Ah rating offered. (In case of external chargers, suitable monitoring of the chargers should be provided in the UPS. Also, all external chargers taking AC input must have PFC - Power factor correction)
12.8	Charger type / Charging Method & Charging Voltages	**Constant Voltage Constant Current** Solid state **SMPS** charger Float Charge 270V±(2V) Boost Charge 280V±(2%V)

12.9	Battery recharge time (After complete discharge) to 90% capacity	10-12 hours
12.10	Battery Housing (Vendor to provide the GA drawings of the offered Battery Rack)	Should be compact and space saving **MS steel open racks** complete with interconnectors
12.11	Battery End Cell Voltage	1.75 V/cell
13	**Interfaces**	
13.1	Serial Communication RS232 Port (Option of USB Port should be available)	RS232 Port should be provided as standard in the UPS. However, there should be provision for USB port also in the UPS.
13.2	REPO(Remote Emergency Power OFF) / ROO(Remote ON - OFF) Port	Provide both onsite & remote EPO to shutdown UPS when emergency situation happens. REPO Port with a user-supplied switch
13.3	Interface to NMS (Network Management System)	SNMP (IPV6) Card for connecting the UPS to LAN thru Ethernet port & monitoring thru NMS should be available (The cost of SNMP Card / NMS software to be quoted separately)
13.4	Interface to BMS (Building Management System) - To be quoted as option	ModBus Card for connecting to UPS to BMS thru RS485 & monitoring thru BMS
13.5	Interface to DCS (Distributed Control System) - To be quoted as option	Relay I/O Card or PFC (Potential free contacts) for connecting to UPS to DCS / PLC / SCADA system for communicating UPS operating status
13.6	UPS status information presented as 3 contact closures	UPS should have configurable input signal as shutdown UPS or battery test dry contact.
14	**Restart / Testing Capability**	
14.1	Cold Start	UPS should start up On AC Supply (Mains) without DC Supply (Batteries) On DC Supply (Batteries) without AC Supply (Mains)
14.2	Automatic Restart	UPS should start up automatically on mains resumption after battery low shutdown
14.3	Self Diagnosis	UPS should be capable to carry out self test of Rectifier / Charger /Battery & Inverter module during start-up
15	**Physical**	
15.1	Operating Temperature	$0℃ \sim 40℃$
15.2	Storage Temperature	$-20℃ \sim 40℃$
15.3	Operating Humidity	$< 95\%$
15.4	Operating Altitude	0 to 3000m(0 To 10000ft)
15.5	Type of Cooling	Forced Air
15.6	Noise Level	$< 60dBA$ at 1 Meter

15.7	Air Filters	UPS should have internal anticorrosion air filters for dust filtration **(Optional)**
15.8	Dimension (w x d x h) in mm	To be furnished by the vendor
15.9	Weight - in kg	To be furnished by the vendor
15.10	Reliability	MTBF greater than 100000 hours
15.11	Packaging Material / Vibration Withstand & Drop Test	Recyclable (No CFC) & 1. Vibration testing as per ISTA -1G Non-operational with Packing
15.12	Standard Package of UPS to include the following minimum accessories	1.SMART Slot 2.MINI Slot 3.Parallel Port 4.RS232 Port 5.REPO Port 6.Charger Detection Port 7.Input Dry Contact 8.Output Dry Contact 9.USB Port
15.13	Parallel Configuration	UPS should have capabilty for parallel 4 units.
15.14	DC bus Capacitor	UPS DC bus capacitor have minimum life of 5 years@40°ambient.
16	**Certifications**	
16.1	Manufacturer	ISO 9001: 2015, ISO 14001: 2015, ISO 18001: 2007
16.2	Product Safety Certifications (Mandatory)	General Safety Requirements for UPS EMC EN/IEC/AS 62040-1 Requirements for UPS EN/IEC/AS 62040-2 UPS Classification according to IEC EN 62040-3 VFI-SS-111
16.3	ROHS compliance	UPS should be ROHS compliance

Intentionally Left Blank

Intentionally Left Blank

2.8. Managed Services

Sl. No.	Item	Description
Network Management Service		
Internet Routing Services		
1		IPv4 subnet allocation
2		Enable routing with peer AS over internet
3		Transit AS services
4		IPv6 subnet Pool allocation
5		IPv6 BGP Peering
Cross Connect and Telco Services		
6		P2P link termination
7		MPLS link termination
8		MPLS connectivity
9		Dynamic routing for achieving auto failovers
10		VRF routing
11		P2P Link with L2TP
Monitoring and Support		
12		Network devices ICMP monitoring
13		CPU, Memory and sessions on Firewall
14		P2P link monitoring
15		MRTG

16		Complete monitoring of network devices, links etc
17		Incident management
18		Problem management
19		Change management
20		Network support
Firewall Services		
21		Standalone Firewall setup
22		Firewalls with HA setups
23		Cable pull test for HA
24		Firewall port opening
25		Firewall port blocking
26		Country wise IP opening or blocking
27		Read-only access to the firewall
28		Trusted SSL certificate import
29		Using the Load balancer feature in Firewalls
30		Policy verification every year
31		IPSEC VPN with Unlimited Users
32		SSL VPN with unlimited users
33		IPSEC remote access VPN with unlimited users
34		Two factor-based authentication Integration
OS Management Service		
35	Windows Server	**OS Installation and Upgrades**
36		**OS Critical and Security Patch Management**
37		**Monitoring of Windows Server.** Monitoring of CPU, RAM, Disk Usage
38		Monitoring of Disk IO, Windows Time Sync,
39		**Monitoring of Windows Server Services**
40		**Monitoring of Windows Server Performance**
41		**Antivirus Patch Management**
42		**Windows Server OS Log Analysis/Management**
43		System, Application and Security Log Analysis

44		**Windows Server Security Management**
45		Security Processes - User and Group Management
46		Security Policies and Configurations
47		Security Patches and Hot Fixes
48		Windows Registry Configurations
49		Windows Services
50		File and Directory Security
51		Audit Logging
52		Windows Firewall Policy
53		Time Zone Setting
54		Event log setting
55		Installation of server feature
		Cluster setup and management
56		Installation/ Modification/ Removal of IIS/ File server role.
57		Configuring disks and volumes includes creating and formatting partitions, logical drives, & volumes
58		Defragmenting volumes to improve file-system performance
59		Managing file-system errors and bad sectors on a hard disk.
60		**Windows Server folder and File access security/ share permission management.**
61		**Windows Server backup Monitoring**
62		Configuring system state and bare metal backup.
63		Restoring system state and bare metal backup.
64		**Windows Server Debug logs and Analysis**
65		**Windows Scheduled Tasks Management** **Windows Server Remote Access Management.**
66		Enable/Disable Remote Desktop
67		Installation/modification/removal of Device Drivers.

68		Create/delete/modify Users and groups
69		Reset password, unlock users
70		**Windows Server Problem/change/incident Management**
71		**24x7 OS Support with Windows Support Service**
Linux OS Management		
72		Installation/ upgrade/ Monitoring of Linux OS
73		Server hardening and uptime monitoring notifications
74		Administration of Linux (SUSE)
75		OS Virtualizations (KVM etc)
76		Cluster setup and management.
77		OS Patching/ Performance tuning/storage migration
78		**Advance Authentication service (LDAP etc)**
79		**Incident/Problem/Change management**
80		**Antivirus management**
81		**Support Service**
Storage management		
82		Break Fix Services (Incident Management)
83		Implementation of Storage with LUN Allocation and management
84		Provide Access to Storage box for customer
85		Manage Access Rights to Storage Volumes
86		Create/delete and Enable/disable Zones on FC Switches
87		Software Patch updates
88		Proactive Monitoring Storage Devices
89		Log Analysis & Reporting
90		Performance Analysis & Tuning
91		Proactive Firmware Upgradation of Disk Drives & Controllers
92		Non Disruptive Storage Migration

93		Capacity Planning & growth Rate Projections. RAID Design & configuration
94		Storage Tiering and thick provisioning
95		Multiple Hot Spares to sustain more than one Disk Failure simultaneously.
96		Enterprise Replication & Snapshots.
97		In-built Non-volatile flash based eternal Cache data protection to sustain power outages.
98		Controller Architecture (Active-Active Symmetric Load balancing Virtualized controllers.)
99		Recommendations on Security Policies
Backup management		
100		Monitoring of backup servers and backup Management
101		Backup Configuration
102		Backup Job Schedule Management
103		Alert Mechanism for Failures
105		Capacity Management
106		Backup Restore Administration
107		Backup Failure Analysis
108		Data Encryption at Transit and at Rest
109		Bare metal Backup
110		Snapshot Backup, Backup on tape
110		Linux Filesystem Backup
111		Windows File System Backup
112		HANA DB, Sybase DB. MAXDB and MS SQL Backup
113		Exchange Backup
114		Tape Lifecycle Management
115		Tape Labeling
116		Tape Rotation
117		Tape Storage in Fire Safe Media Rack
118		Tape Retrieval from Tape Drives
119		Tape Collection within Municipal Boundary

120		Physical Verification and Audit of Media
VMWare Services		
120	Monitoring/configuration of ESXI Services	CPU, RAM & DISK
121		Memory Overcommitment
122		Unlimited Virtual SMP
123		Hot Pluggable Virtual HW
124		MPIO / Third-Party Multi-Pathing
125		Memory Ballooning/NIC teaming
126		Installation/Modification/Deletion of ESXi device Drivers
127		Esxi Server Log Analysis/Management.
128		Security Processes - User and Group Management
129		vSphere Host Profiles
130		Authentication Services
131		Security Profile
132		Audit Logging Requirement
133		ESXi Firewall Policy
134		Time Zone Setting
135		Sys Log Settings
136		Managing vSphere Plugins
137		vSphere Update Manager
138		vSphere Dump Collector
139		vSphere Management Assistant
140		vCenter Management
142		SMTP Email Alerts
143		vSphere Web client
144		vSphere HA, DRS, SDRS, FT, vMotion, Storage vMotion
145		vSphere API, Storage API
147		vSphere DPM
148		Datastore & Datastores Clusters

149		vCenter Server Appliance
150		Inventory Extensibility
151		vCenter Single Sign-on
152		Linked Mode,
153		Custom Roles and Permissions
154		Improved large-scale management
155		VMWare vRealize Orchestrator, VMWare vRealize Operations Standard
156		Proactive Optimization
157		Dynamic Allocation of Resources – DRS
158		Resource Management, Managing Scheduled Tasks., Analyzing ESXi Host debug logs.
159		P2V and V2V Migration
160		ESXi OS Critical and Security Patch Management
Security Management		
161		OS Logs, AV/AS logs, Vulnerability Assessment, Network Device Logs, Rule Based Correlation & Risk Based Correlation
162		Incident Management, Log Retention for 6 Months
163		Penetration Testing (Tool based)
164		Historical Based Correlation
165		PCI DSS, FIM, Advanced Persistent Threat protection, IPS/IDS, DDOS Protection, DDOS Reporting, Enabling DDOS services for NMDC networks
166		Basic web filter service
167		Application filter services
168		Automatic updates of signatures
DC-DR Services		
169		RTO - Recovery Time Objective <-4 Hours RPO – Recovery Point Objective <= 30 Minutes
170		Network Convergence and Recovery

171		Failback and Primary DC Restoration
172		DNS/GSLB
173		Application Recovery

2.9. NOC

i) Desktop for NOC

Sr. No.	Description	
1	Make & Model Offered	To be clearly mentioned. All the relevant product brochures and manuals must be submitted
2	Processor: 5th Generation Intel Core i5 or above.	
3	Operating System: Windows 10 Prof. or above (64 bit).	
4	Display: 23 inch or above HD	
5	Port: HDMI, USB	
6	Memory (in GB): 8 or higher	
7	Hard Drive: 1 TB 5400 rpm	
8	Graphics Card: 2 GB Graphics Card make NVIDIA GeForce, ATI Radeon or equivalent	
9	DVD- R/W	
10	MS Office Standard License	

ii) Screen/ Console (Large Format Display)

Sl. No.	Description	
1	Make & Model Offered	To be clearly mentioned. All the relevant product brochures and manuals must be submitted
2	LFD shall be of 55-inch, full HD, 2 HDMI Ports, 1 VGA Port with AV features, 1 USB min, Contrast 4000:1	

1.0   __Optical Fibre Laying:__

The Executing Agency shall prepare and submit for approval by the Purchaser, specific construction drawings for all types of soil strata/crossings taking into consideration the guidelines given in this specification. The construction/implementation shall be carried out as per the approved drawings.

The construction drawings shall inter-alia include the longitudinal sectional diagram of the trench for different soil strata and detail arrangement of crossings, number of pipes, size of pipe, locations and position of manholes, other details as per the technical specifications. Route maps shall be drawn to the scale of 1:20,000. For convenient handling in the field, the map shall be made on 300mm(W) and lengths not exceeding 1190mm sheets with 30 mm overlap shown on subsequent sheets.

1.1 Clearances

The Executing Agency shall be responsible for obtaining necessary clearances for excavation work from the authorities on behalf of the Owner and provide requisite copies of information, maps, survey report etc to the authorities. The Owner/Employer shall assist the Contractor in obtaining such clearances by providing the authority letter or any other relevant document. The Contractor shall make an all out effort with the concerned authority to get clearances expeditiously and to negotiate the least cost to the Owner/Employer. The Owner/Employer shall furnish all required bank guarantees and make payments to the concerned authorities directly based on the demand letter obtained by the Contractor from the concerned authorities. The Contractor shall ensure quick and speedy clearances in order to implement the project within stipulated schedule. In case the authorities have some objections on certain sections of routes proposed and are unwilling to provide clearances, the Contractor shall propose an alternate route, promptly carry out the survey and submit specific survey report for that and reapply for clearance after taking into account the comments/objections of the authority.

1.2   Excavation and Backfilling

The Contractor shall carry out excavation and backfilling of trenches in all kinds of soil strata such as normal soil, soft rock, hard rock for laying PLB HDPE pipe, RCC hume pipe and GI pipe.
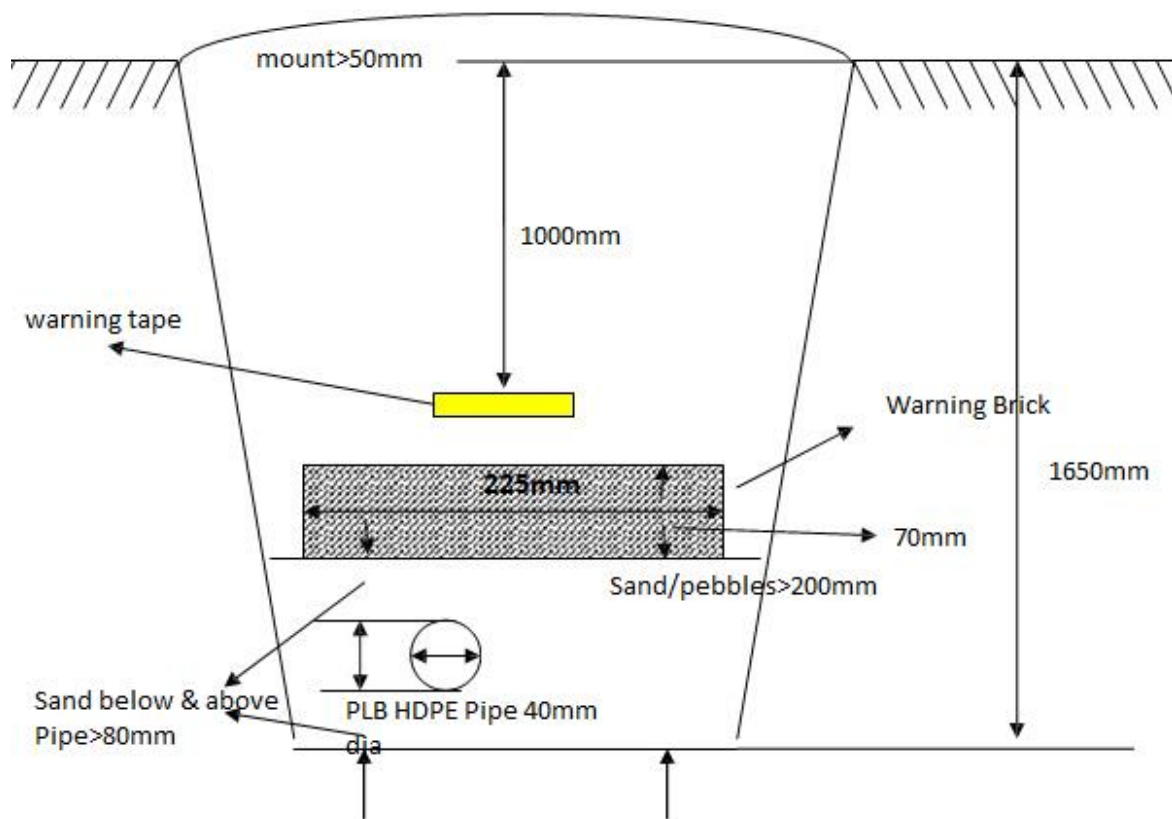
Figure 1.0: Trench in Normal Soil for 1 PLB HDPE pipes (Not To Scale)

1.2.1 Excavation

The cable trenches shall be dug as per route plan and detail trench drawings (indicating the various dimensions and other details of the trench) approved by the Owner/Employer for each type of soil strata. The Contractor shall take due care and precaution during excavation to avoid possible damage of other underground plants/facilities in the proposed underground fibre optic cable route and shall indemnify the Owner/Employer for all damages and shall be solely responsible for all the damages and losses. The Owner/Employer shall not be liable for any damages/losses.

For the purpose of this specification, soil strata types are defined below:

Normal Soil   All type of soil {i.e. dry, wet (partially or fully submerged)} except soft rock or hard rock as defined below.

Soft Rock   Lime stone, laterite, hard conglomerate or other fissured rock   which can be quarried or split with crow bars, wedges or pickaxes. However, if required light blasting may be resorted to for loosening the material, but this will not in any way entitle the material to be classified as hard rock.

Hard Rock   Any rock excavation other than specified under Soft Rock, for which blasting, drilling, chiseling are required.

Depth of trench shall be at least 1650 mm in normal soil. However, for rail & road crossings the trench depth shall be at least **1000** mm. Depth of trench shall be at least 1000 mm in soft rock from the depth softrock is encountered i.e. in case soft rock is encountered at say 500 mm then the actual depth of the trench shall be 500+1000 = 1500 mm limited to a maximum depth of 1650mm. Depth of trench shall be at least 800 mm in hard rock from the depth hard rock is encountered i.e. in case hard rock is encountered at say 300 mm then the actual depth of the trench shall be 300 + 800 = 1100 mm limited to a maximum depth of 1650mm. For excavation in hard rock, controlled blasting can be resorted to. The Contractor shall obtain necessary permissions from the statutory authorities for blasting and the use of explosives for this purpose. No blasting is permitted near permanent work or dwellings. Blasting shall be so made that pits are as near to the designed dimensions as practicable. Jackhammers can also be used for the excavation. The width of trench at the top and bottom shall be adequate for proper installation of PLB HDPE pipes, RCC hume pipes, GI pipes Warning tape, route marker and joint markers. The contractor shall submit the construction drawing for approval. The trench depth shall be measured from the bottom of the trench. Trench shall be located at the lowest point of lower area if possible. Trench shall not be constructed at field boundary or any up-heap. In case of uneven ground, the Contractor ensure that the bottom of the trench is not uneven, the Contractor shall maintain minimum depth of the trench as per specifications and may be required to increase the depth at some locations and provide a suitable gradient in the trench.

During the construction of trenches, the Contractor shall be responsible for shoring and strutting the walls of the trench on either side by using suitable means such as wooden planks to avoid subsidence of soil. The Contractor shall also be responsible for supporting the exposed plant/facilities of other utilities such as water, gas and oil pipes, electric, telephone or fibre optic cables etc. to avoid any possible damage. The Contractor shall also be responsible for any dewatering of the trench during digging and installation of pipes.

In case it is necessary to get around a large obstacle such as a boulder or an underground plant/facility, which has not been anticipated earlier the trench may be given a gentle bend within permissible radius or by construction of a manhole. Wherever possible, it is preferable to avoid additional manholes.

The **Purchaser Project Manager or his/her authorized representative** will be the authority to decide the classification of the soil i.e. normal soil, soft rock or hard rock. In few cases where the

required depth is not achievable, the Project manager may allow the lesser depth subject to providing the suitable protection such as providing the concrete casing of the installed ducts. For such cases, the contractor shall propose the suitable protection arrangement along with the reasons for non-achievability of the required depth and obtain the specific approval of the project manager before execution of the work. The decision of the Project Manager shall be final and binding on the Contractor.

1.2.2 Backfilling

After installation of PLB HDPE pipes, RCC hume pipes or GI pipes, the backfilling of the trench shall be done. The PLB HDPE pipes shall be sandwiched with sand as per the Figures 1.0. Backfilling shall normally be done with the excavated soil, unless it consists of large boulders/stone in which case the boulders/stone shall have to be broken to a maximum size of 80mm. The backfilling should be clean and free from organic matter or other foreign material. The earth shall be deposited in maximum 200 mm layers levelled and wetted and tamped properly before another layer is deposited. The earth filling is done with a suitable mount to allow for any shrinking of soil at the later date. In case of regular footpath, temporary reinstatement shall be done after backfilling. The left out earth if any has to be disposed by the Contractor to a suitable location as indicated by authorities at his own cost. It is advisable to start backfilling of the trench from one end or after padding of the pipe to avoid uplifting. In case of soft rock as well as hard rock, the PLB HDPE pipe shall be covered with 1:2:4 concrete. The cross section of the concrete shall be 100 mm (depth) x 200 mm (width). The Contractor shall properly cure the concrete for four days. The backfilling of the remaining portion shall be done as stipulated for normal soil.

Final inspection of the backfilling shall be done jointly by the Executing Agency and Purchaser immediately after first monsoon and the Executing Agency shall rectify the defects, if any, without any cost to the Purchaser.

1.3   Marking

The Contractor shall provide markers, warning bricks and warning tape as stipulated below for the routes where new PLB HDPE pipes are installed under this package.

A)   Markers

Route markers made of RCC (1:2:4) of length 1450 mm and a bottom cross section of 150mmx200mm tapering to 75mmx125mm at top shall be provided. Route markers shall be provided at 500 mm from the trench and away from the road centre, at an average of 200 m. Markers shall also be provided at major directional changes in route (from straight) and at both sides of all types of crossings. 900 mm of the marker shall be underground and 550 mm shall

be above the ground. The portion of route markers above ground shall be painted with brown synthetic enamel paint.

Joint Markers shall be provided at each joint location and shall be same as route markers except that they shall be blue in colour. In case joint markers and route markers fall at the same location, route marker shall not be installed and only joint marker shall be provided.

All Markers shall be Engraved vertically as "NAME OF UTILTIY" in 500 mm portion above the ground area and filled with fluorescent white colour. The marking shall face the road.

B)   Warning Bricks

Bricks class designation-5(50) of the actual size 225 mm (Length) x 111 mm (Width) x 70 mm (Thick) shall be laid breadth-wise as per the slandered practice (average 9 bricks per meter) in city area (municipality limits) immediately above the sand layer in which PLB HDPE pipe is installed. Stone slabs of suitable size may also be used in place of warning bricks with the approval of the Owner/Employer.

C)   Warning Tape

A warning tape, made of HDPE or LDPE (Low Density Poly Ethylene) other suitable inert material, containing a printed message "**WARNING :" Name of utility's " Fibre Optic Cable below**" shall also be laid over the pipe, throughout the cable route at a depth of 1000mm in normal soil (the depth in soft rock and hard rock shall be proposed by the Contractor and approved by the Owner/Employer), for warning the person who is excavating the trench. The width of the tape shall be at least 100 mm and thickness of the tape shall be at least 500 micrometers. The life of the warning tape shall be at least 25 years.

1.4   Installation of PLB HDPE Pipe

Two PLB HDPE pipes two PLB HDPE pipes **(one spare for future use)** shall be laid. Two PLB HDPE pipes shall be laid side by side (minimum spacing 30 mm) at bottom of the trench after making the surface smooth and providing 80 mm of sieved, stone free sand bedding. After laying the pipe additional sieved sand shall be added to increase the height of the sand layer to a total of 200 mm hence positioning the PLB HDPE pipe in the middle of the layer. In case of unavoidable rat infected areas along the finalised route, pebbles of dia 20 mm (nominal) shall be used in place of the sand. Other important steps are described as under:

   a. PLB HDPE Pipe shall be laid in a flat bottom trench free from stones, sharp edged debris. Pipe shall not be laid in water filled trenches.

b. The Pipe shall be placed in trenches as straight as possible. Minimum bending radius of pipe and fibre optic cable shall always to be taken into account.

c. The ends of pipes shall always be closed with end plugs to avoid ingress of mud, water or dust i.e. all pipe opening shall be sealed to avoid entry of foreign material.

d. The pipes shall be joined tightly & properly through plastic couplers and the joint shall be smooth and free from steps. The joints shall be made properly so that it passes the duct integrity test. All joints shall be assembled with proper tools only.

e. Coupler shall not be placed along the bend portion of the pipe and hacksaw shall never be used to cut the pipe.

f. Cable sealing plugs shall be provided at all manhole locations and at locations cable is coming out of the pipe and empty pipe ends i.e. all pipe openings shall be sealed to avoid entry of foreign objects.

g. PLB HDPE pipes shall be installed in a manner that fibre optic cable can be pulled, blown, de- blown without damaging the fibre optic cable due to stresses.

The Executing Agency shall get inspected, by a representative of Purchaser, all joints before carrying out the backfilling. Joints shall be visually inspected and checked for tightness.

1.5   Reinstatement

The Executing Agency shall be required to carry out reinstatement of the excavated area in case the concerned authority requires so. Reinstatement shall include all works necessary (such as reconstruction of metalled/asphalt road, footpath etc) to restore the excavated area to original quality and shape.

1.6   Underground Fibre Optic Cable Installation

The cable shall be installed inside one of the 40mm diameter PLB HDPE pipes installed under this package along the route(s). The cable shall be installed by compressed air blowing technique. The cable blowing machine shall be suitable for blowing the proposed section lengths of fibre optic cables.

As various utilities have already installed their fibre optic cables in the existing PLB HDPE pipe routes, the Contractor shall take due care and precaution during installation of fibre optic cable and the rectifications work to avoid possible damage of ducts / OFC of other utilities. The Contractor shall indemnify the Owner/Employer for all the damages and the Contractor shall be solely responsible for the damages and losses. The Owner/Employer shall not be liable for any such damages.

Executing Agency shall provide armored fibre optic cable (TEC approved design) in some of the sections, which are not suitable for unarmored cable installation in ducts (example: highly rat infected sections). The armored fibre optic cable shall also be installed inside the PLB HDPE pipe / GI pipe / RCC pipe, as applicable. The routes and types of installation shall be finalised during project execution based on the site survey report and actual requirements.

The Contractor shall propose the exact methods and procedures for installation taking into consideration the following guidelines, for approval by the Owner/Employer.

a. The Optical Fibre Cable Drums shall be handled with utmost care. The drum shall not be subjected to shocks by dropping etc. They shall not be normally rolled along the ground for long distance and when rolled, shall in the direction indicated by the arrow. The battens shall be removed only at the time of actual laying.
b. A blowing machine in association with an appropriate compressor shall be used for blowing.
c. Temporary blowing chambers (if required) shall be constructed and then backfilled after blowing operation is completed.
d. Locations along the route, which provide easy access points for blowing machine and compressor, shall be determined.
e. Before starting the cable blowing, both PLB HDPE pipes installed under this package shall be checked for obstacles or damage. The already installed PLB HDPE pipe wherein cable are to be installed under this package shall also be checked for obstacles or damage. Checking shall be done by using a proper sized mandrel equipped with a transmitting device.
f. Always blow downhill wherever possible.
g. Multiple blowing machines may be used in tandem if so required.

Installation by pulling may be permitted by the Owner/Employer in specific cases where installation by blowing is not feasible. In case pulling is used, the pulling speed shall be determined considering the site condition. Care must be taken not to violate the minimum bending radius applicable for the fibre optic

cable. Tension in the cable during laying shall not exceed tension limit of the offered FO cable and the cable should not be damaged during or after the pulling. While installing the cable, excess length of about 10 meters shall be stored at each joint location for each side. Excess length of 10 m shall be kept at one ends of a road crossing, culvert crossing and 20 meters at one end of bridges.

1.7 Trenchless Digging

Trenchless digging may be used in short section for crossing National highways, important road or rail crossings etc., where the concerned authorities do not permit open cut method, for which no additional cost shall be provided by the Employer.

Section B: Foundation Details for Relocatable Standard Pole
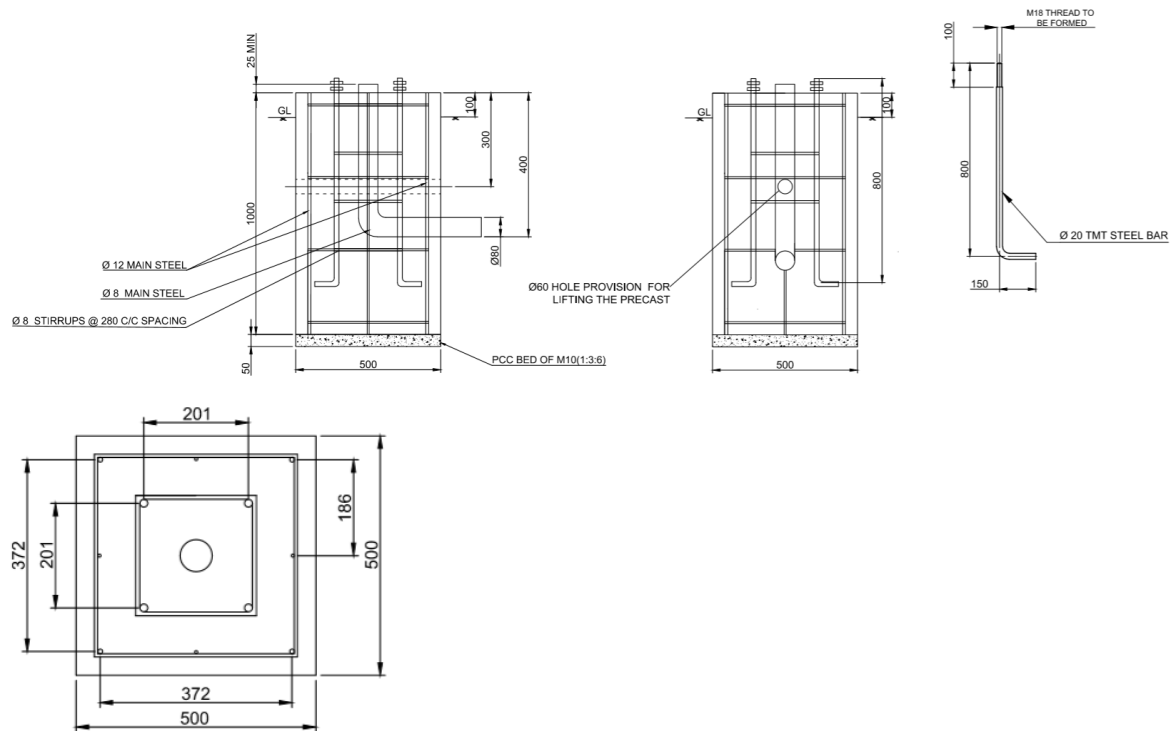
1. P.C.C. Bed of M10 (1:3:6) Concrete 50 Thick to be laid below foundation
2. Foundation to be made of RCC with M20 Concrete
3. Anchor/J-Bolts to be made from Dia 25 TMT Steel Bars and bent as shown in figure and to be threaded M20X80 on end and galvanized
4. Dia 10 TMT Steel Bars stirrups at 200 C/C spacing to be provided for J bolts
5. 80 PVC pipe with elbow/HDPE pipe to be inserted withing the cage formed for cable entry as shown and to be accommodated within the space without disturbing the stirrups
6. PVC pipe with elbow should have min. 60 clearance after concreting at both ends
7. 8 nos. M20 Galvanized Steel nuts and 8 nos. M20 Galvanized Steel washers are to be used for Pole installation
8. The grouted J-bolts position should match with the Base Plate of the Relocatable vertical pole assembly
9. M20 concrete is used for RCC works
10. 50 mm cover is provided for main bars

Annexure-VI

DC Hardware Description	Make	Model	Quantity (Q)	HSN Code	Unit Price in Rs.(P)	Total Pirce In Rs. (QxP)
SAP HANA Appliance S/4 — 3 TB			2			-
SAP HANA Appliance SRM — 1.5 TB			2			-
SAP HANA Appliance BW — 1.5 TB			2			-
SAP HANA Appliance for Dev — 768 GB			1			-
SAP HANA Appliance for Quality - 3 TB			1			-
OS Cluster software (Note : Quantity as applicable)						-
Blade Enclosure (as per OEM solution for 24 blades)						-
(Note : Quantity as applicable)						
Blades for Application Servers - SAP Environment			10			-
Blades for ADS, Mail,Backup & Misc Servers			4			-
Blades for EMS Servers in HA 2+2			4			-
SAN Storage			1			-
SAN Switches			2			-
Backup Device with Backup SW for disk backup			1			-
Tape Library with backup SW			1			-
DataCentre Core Switches			2			-
ToR Switch 24 SFP+ for DC			4			-
1G Copper Switch for SAP HANA Backup — 24 ports			1			-
1G copper switch for Management — 48 ports			2			-
Blades for Legacy Servers			6			-
Installation Charges - Lumpsum			1			-
					Total (A) in Rs.	**-**

DR Hardware Description	Make	Model	Quantity (Q)	HSN Code	Unit Price in Rs.(P)	Total Pirce In Rs. (QxP)
SAP HANA Appliance DB — 3 TB			1			-
SAP HANA Appliance SRM — 1.5 TB			1			-
SAP HANA Appliance BW — 1.5 TB			1			-
Blade Enclosure (as per OEM solution for 11 blades)			1			-
Blades for Application Servers - SAP Environment			5			-
Blades for ADS, Mail, Backup & Misc Servers			2			-
SAN Storage			1			-
SAN Switches			2			-
Backup Device with Backup SW for disk backup			1			-
Core Switches			1			-
ToR Switch for DR - 24 SFP+			2			-
1G copper switch for Management — 48 ports			1			-
Installation Charges - Lumpsum			1			-
					Total (B) in Rs.	-
					Grand Total in Rs.	**-**

Note 1: Applicable tax rates should be mentioned.

Note 2: All line items to be quoted. If any line item not indicated with price, the same will be considered as free of cost supply and PO placed accordingly.

Name of the supplier:
Mail Id:
Mobile:

Annexure-VI

DC Software Description	Make & Model	Quantity (Q)	HSN Code	Unit Price in Rs.(P)	Total Pirce In Rs. (QxP)
Operating System for App Servers	SUSE Linux for SAP 2Skt Unlimited Guest with HA	10			-
OS for ADS, Mail,Backup & Misc Servers	WinSvr STD 2019 OLP Core Licenses	4			-
OS for EMS Servers	WinSvr STD 2019 OLP Core Licenses	4			-
Virtualization SW	VMWare vCentre Standard with 5 yrs	1			-
	VMWare vSphere Enterprise Plus with 5 yrs	48			-
OS for HQ & Plant Servers	WinSvr STD 2019 OLP Core Licenses	3			-
OS for HQ & Plant Servers	SUSE Linux for SAP 2Skt Unlimited Guest OS	3			-
EMS	Enterprise management software	1			-
Microsoft Active Directory CAL licenses	Microsoft & Active Directory	1000			-
Installation Charges - Lumpsum		1			-
				Total (A) in Rs.	-

DR Software Description	Make & Model	Quantity (Q)	HSN Code	Unit Price in Rs.(P)	Total Pirce In Rs. (QxP)
Operating System for App Servers	SUSE Linux for SAP 2Skt Unlimited Guest OS	5			-
OS for ADS, Mail,Backup & Misc Servers	WinSvr STD 2019 OLP Core	2			-
Virtualisation SW	VMWare vCentre Standard with 5 yrs	1			-
	VMWare vSphere Enterprise Plus with 5 yrs	14			-
Installation Charges - Lumpsum		1			-
				Total (B) in Rs.	-
				Grand Total in Rs.	-

Note 1: Applicable tax rates should be mentioned.
Note 2: All line items to be quoted. If any line item not indicated with price, the same will be considered as free of cost supply and PO placed accordingly.

Name of the supplier: 0
Mail Id: 0
Mobile: 0

Annexure-VI

Local XMII **Software Description**	Make & Model	Quantity (Q)	HSN Code	Unit Price in Rs.(P)	Total Pirce In Rs. (QxP)
Operating System for xMII Servers	SUSE Linux for SAP 2Skt Unlimited Guest OS	6			-
ADS, Antivirus & Patch Mgmt Servers operating system	Windows server 2019 standard operating system	6			-
Installation Charges - Lumpsum		1			-
				Total (A) in Rs.	-

Local XMII **Hardware Description**	Make	Model	Quantity (Q)	HSN Code	Unit Price in Rs.(P)	Total Pirce In Rs. (QxP)
xMII Rack Servers			6			-
ADS, Antivirus & Patch Mgmt Servers (Rack servers)			6			-
Installation Charges - Lumpsum			1			-
					Total (B) in Rs.	-
					Grand Total in Rs.	**-**

Note 1: Applicable tax rates should be mentioned.
Note 2: All line items to be quoted. If any line item not indicated with price ,the same will be considered as free of cost supply and PO placed accordingly.

Name of the supplier: 0
Mail Id: 0
Mobile: 0

Annexure-VI

Firewall BoM

Sr. no.	Description	Make	Model	UoM	Quantity (Q)	HSN Code	Unit Price in Rs.(P)	Total Pirce In Rs. (OxP)
	WAN Network Interface Firewalls : Accepted Makes: Fortinet, Palo Alto, Cisco with 5 Year Support							
1	Firewall-Type 1			Nos.	2			-
2	Firewall-Type 2			Nos.	11			-
3	Firewall-Type 3			Nos.	6			-
4	Firewall-Type 4			Nos.	4			-
5	Firewall-Type 5			Nos.	20			-
6	Firewall- Web Application Firewall			Nos.	2			-
7	Centralized Management, Log and analysis license with 5 - year support up to 100x firewall devices/administrative, supplied along with 5 years 24 x 7 support along with hardware sppliance			Nos.	1			-
8	Free of change training to 20-people team of Network Engireers from NMDC to be provided by OEM at a centralized place covering all aspects of operations and maintenance of the firewalls			Nos.	1			-
9	Installation and Commissioning charges for the above			Lumpsum	1			-
							Total	-

Note 1: Applicable tax rates should be mentioned.
Note 2: All line items to be quoted. If any line item not indicated with price, the same will be considered as free of cost supply and PO placed accordingly.

Name of the supplier: 0
Mail Id: 0
Mobile: 0

Annexure-VI

Switch BoM

| Sr.no.		Make	Model	UoM	Quantity (Q)	HSN Code	Unit Price in Rs.(P)	Total Pirce In Rs. (QxP)
	Ethernet Switches and Access Points. Accepted Makes: Extreme, HPE, Cisco with 5 years support							
1	CoreSwitch - Type 1			Nos	6			-
2	CoreSwitch - Type 2			Nos	1			-
3	10G-ER SM SFPs for distribution switches to core Switches Links			Nos	8			-
4	10G-LR SM SFPs for distribution switches to Access and Distribution Switches			Nos	64			-
5	Distribution Switch - Type 1			Nos	7			-
6	Distribution Switch - Type 2			Nos	11			-
7	1G-LX SM SFPs for distribution Switches to Access Switches Links			Nos	478			-
8	10G-LR SM SFPs for distribution Switches to access Switches Links			Nos	200			-
9	1000BASE-T RJ45 SFP Transceiver			Nos	20			-
10	Access Switch - Type 1			Nos	305			-
11	Access Switch (Industrial Grade) - Type 2			Nos	153			-
12	Access Point (indoor)			Nos	300			-
13	Wireless LAN Controller for Access Points 5 year warranty & NBD support			Nos	10			-
14	NAC Licenses for switches and access points, 5 year warranty & NBD support			Nos	6			-
15	EMS for Intergrated Mointoring of (Industrial, Access, Distribution and Core) Switches and Wirless Access Points, 5 years NBD support			Nos	6			-
16	VM for installation of NAC and EMS - 4 CPU x 86 corces, 64MB RAM, 500 GB x2 disks in failover RAID			Nos	6			-
17	Free of charges training to 20-people team of Network Engineers from NMDC to be provided by OEM at a centralized place covering all aspects of operations and maintenance of the switches. Aps. NAC, WLC, EMS			Nos	1			-
18	Installation and Commissioning charges for the above			Lumpsum	1			-
							Total	-

Note 1: Applicable tax rates should be mentioned.
Note 2: All line items to be quoted. If any item not indicated with price, the same will be considered as free of cost supply and PO placed accordingly.

Name of the supplier: 0
Mail Id: 0
Mobile: 0

Annexure-VI

Wifi

Outdoor Wi-Fi Zone - Accepted Make: Cambium, Ruckus, Cisco, Aruba, Radwin

Sl. No.	At Dumper Platforms, PoL and Workshops	Make	Model	UoM	Quantity (Q)	HSN Code	Unit Price in Rs.(P)	Total Pirce In Rs. (QxP)
1	Outdoor (IP66 or better rated) 90-120 sector 802.11 ac WLAN AP with Tilt bracket & PoE Injector, 5-year extended warranty to be included. AP with set of 2 antenna (for 240-degree coverage) to be included			Nos.	58			-
2	Supply & Installation of Tower / Pole, 5m, Galvanized steel, with grouting base and accessories with Lightning Arrestors			Nos.	29			-
							Total(A)	-
	P2P Radio Links (for Workshop @ Bacheli)							
1	5 GHz PTP Radio, Integrated High Gain Antenna (ROW) with **power lead**, 5-year extended warranty, IP66 or better rated			Nos.	6			-
2	Coaxial Cable Grounding Kits for 1/4" and 3/8" Cable			Nos.	12			-
3	LPU and Grounding Kit (1 kit per ODU)			Nos.	6			-
4	POWER SUPPLY, 30W, 56V - Gbps support			Nos.	6			-
5	Tilt Bracket Assembly			Nos.	6			-
6	Supply & Installation of Tower / Pole, 15m, Galvanized steel, with grouting base and accessories with Lightning Arrestors			Nos.	3			-
							Total(B)	-
	Wi-Fi Zones and P2P links for mine coverage (Shovels, Dozers etc.) & weighbridges at KIOM							
	Wi-Fi Zones							
1	Outdoor (IP66 or better rated) 90-120 sector 802.11ac WLAN AP with Tilt bracket & PoE Injector, 5-year extended warranty to be included. AP with set of 2 antenna (for 240-degree coverage) to be included			Nos.	84			-
2	Supply & Installation of Tower / Pole, 5m, Galvanized steel, with grouting base and accessories with Lightning Arrestors			Nos.	28			-
							Total(C)	-
	P2P Links							
1	Coaxial Cable Grounding Kits for 1/4" and 3/8" Cable			Nos.	92			-
2	LPU and Grounding Kit (1 kit per ODU)			Nos.	46			-
3	5 GHz PTP Radio, Integrated High Gain Antenna (ROW) with **power lead**, 5-year extended warranty, IP66 or better rated			Nos.	46			-
4	POWER SUPPLY, 30W, 56V - Gbps support			Nos.	46			-
5	Tilt Bracket Assembly			Nos.	46			-
6	1 PPS GPS Sync generator			Nos.	46			-
7	PoE Gigabit DC injector, 15W Output at 30V, Energy Level 6 Supply			Nos.	46			-
8	Supply & Installation of Tower / Pole, 15m, Galvanized steel, with grouting base and accessories (some will be mounted on Wi-Fi zone towers)			Nos.	17			-
9	Free of charge training to 20-people team of Network Engineers from NMDC to be provided by OEM at a centralized place covering all aspects of operations and maintenance of the Outdoor WAPs			Nos.	1			-

	Description	Unit	Qty		Rate	Amount
1	PMP Radio, IP66 or better rated, 240-degrees coverage (may need 2 base stations if each unit provides only 120-degree coverage), with all accessories and 5-year extended warranty.	Nos.	5			-
2	Remote radios for the PMP, 4 radios per zone, 240-degree coverage with all accessories and 5-year extended warranty.	Nos.	20			-
3	Supply & Installation of Tower / Pole, 5m, Galvanized steel, with grouting base and accessories, with Lightning arrestors	Nos.	25			-
4	Supply & Installation of 15m Tower (3-legs), with all accessories for outdoor-Wi-fi AP installation, with Lightning arrestors	Nos.	5			-
	Installation and Commissioning charges for all of the above BOM's	Lumpsum	1			-
					Total(E)	-
					Grand Total (A+B+C+D+E)	-

Note 1: Applicable tax rates should be mentioned.
Note 2: All line items to be quoted. If any line item not indicated with price, the same will be considered as free of cost supply and PO placed accordingly.

Name of the supplier: 0
Mail Id: 0
Mobile: 0

Annexure-VI

Campus Backbone Cabling - Accepted Makes: CommScope Netconnect, Belden, Corning, Cmon

S.No	Item Description	Make	Model	Units	Quantity (Q)	HSN Code	Unit Price in Rs. (P)	Total Pirce In Rs. (QxP)
1	12-Core SM double jacketed Outdoor armored cable			Meters	189500			-
2	6-Core SM double jacketed Outdoor armored cable			Meters	80500			-
3	48-fiber 2U, rack mounted fiber optic patch panels, for terminating OSP cables, with fusion splice trays, fully loaded with Duplex-LC SM adapters and 48 numbers of LC SM pigtails (48 numbers per panel)			Nos.	50			-
4	24-fiber 1U rack mounted fiber optic patch panels, for terminating OSP cables, with fusion splice trays, fully loaded with Duplex-LC SM adapters and 24 numbers of LC SM pigtails (24 numbers per panel)			Nos.	234			-
5	LC-LC Duplex SM Patch Cords, 3 meter			Nos.	626			-
							Total(A)	-
Closed Steel Racks -								
1	42U Racks as per specifications with vertical 2 PDUs, SNMP enabled (for Core Switches)			Nos.	11			-
2	42U Racks as per specifications with vertical 2 PDUs, surge protected (for Distribution Switches)			Nos.	21			-
3	24U Racks as per Specifications, with horizontal PDUs (IP Rated)			Nos.	153			-
4	24U Racks as per Specifications, with horizontal PDUs only (Non-IP Rated)			Nos.	227			-
							Total(B)	-
	Horizontal Cabling - Accepted Makes: CommScope Netconnect, Belden, Panduit							
1	1U, 24-port Cat6A UTP Unloaded Jack Panel with rear Cable Support bar			Nos.	9			-
2	Cat6A UTP Patch Cord (7-feet)			Nos.	462			-
3	Cat6A UTP Information Outlet at DC Rack End			Nos.	362			-
4	1-port Face Plate			Nos.	161			-
5	45mm x 45mm Backbox			Nos.	130			-
6	IP rated Backbox for Faceplates and Information Outlets			Nos.	50			-
7	Cat6A UTP Cable			(305 Mtr.) Roll	20			-
8	Plugs for Modular Plug Terminated Links, for Wi-Fi APs and CCTV			Nos.	275			-
9	Cat6A UTP Information Outlet at End-User Rack End			Nos.	100			-
							Total(C)	-

Horizontal Cabling - Accepted Makes: CommScope Netconnect, Belden, Panduit

#	Description	Units	Quantity (Q)	HSN Code	Unit Price in Rs.(P)	Total Pirce in Rs. (QxP)
1	1U, 24-port Cat6 UTP Unloaded Jack Panel with rear Cable Support bar	Nos.	234			-
2	Cat6 UTP Patch Cord (7-feet)	Nos.	5600			-
3	Cat6 UTP Information Outlet at DC Rack-End	Nos.	2800			-
4	1-port Face Plate	Nos.	1401			-
5	45mm x 45mm Backbox	Nos.	982			-
6	IP rated Backbox for Faceplates and Information Outlets	Nos.	510			-
7	1 Port Surface Mount Box	Nos.	1294			-
8	Cat6 UTP Cable	(305 Mtr.) Roll	472			-
9	Cat6 UTP Information Outlet at End-User Rack-End	Nos.	2800			-
10	Installation and Commissioning charges for the above	Lumpsum	1			-
	Total(D)					-

UPS - Suggested Makes: APC, Emerson or equivalent	Units	Quantity (Q)	HSN Code	Unit Price in Rs.(P)	Total Pirce in Rs. (QxP)
1 Supply, Installation, Testing and Commissioning of 1 KVA UPS system (prefer 19' rack mountable unit) for Distribution and access Switches at Bacheli, Kirandul, Donimalai, Panna and Paloncha. 1KVA rating, SNMP manageable. Supply should include 30-minute battery back-up batteries of 65AH, 12V, SMF related electrical protection accessories and rack, 3-year on-site warranty and maintenance	Nos.	259			-
2 Supply, Installation, Testing and Commissioning of (N) 30KVA UPS System for Central Distributor to support core switches, Servers, WAN Optimizers, ILL load balancers, and other networking equipment along with 30-minutes battery back-up (about 40 batteries of 65AH, 12V, Lead Acid, SMF) along with Battery rack, MCB protection gear and all other accessories - Bacheli, Kirandul, Donimalai, Panna and Paloncha. UPS to be SNMP manageable. 30kVA rating. Supply should include 3-year on-site warranty and maintenance	Nos.	5			-
3 Supply & Installation of Grounding Pit and services- for servers and communication	Nos.	14			-
4 Supply & Installation of Lightning arrestors and grounding pit	Nos.	14			-
5 Installation and Commissioning charges for the above	Lumpsum	1			-
Total(E)					-

Installation of Cable Links		Units	Quantity (Q)	HSN Code	Unit Price in Rs.(P)	Total Pirce In Rs. (QxP)
1	Installation of Racks, Earthing etc.	Nos.	412			-
2	Installation, Testing and Commissioning of Horizontal Cable Links along with supply of requisite Caping & Casing / PVC conduits / HDPE pipes	Nos.	3162			-
					Total(F)	-
					Grand Total(A+B+C+D+E+F)	-

Note 1: HDPE ducts will be supplied by ITI and rates need not be quoted.
Note 2: Applicable tax rates should be mentioned.
Note 3: All line items to be quoted. If any line item not indicated with price, the same will be considered as free of cost supply and PO placed accordingly.

Name of the supplier: 0
Mail Id: 0
Mobile: 0

Annexure-VI

OFC Laying	Make	Model	UoM	Quantity (Q)	HSN Code	Unit Price in Rs.(P)	Total Pirce In Rs. (QxP)
1	Installation (Trenching, cable pulling through HDPE pipes, Manholes every 2kMs or 2 right angle bends) Testing and Commissioning of Optical Fibre Links along with supply of ISI marked / TEC approved HDPE pipe		Meters	270000			-
2	Splicing & testing of OFC (Pigtails)		Nos.	284			-
						Total	-

Note 1: Applicable tax rates should be mentioned.

Note 2: All line items to be quoted. If any line item not indicated with price, the same will be considered as free of cost supply and PO placed accordingly.

Name of the supplier: 0
Mail Id: 0
Mobile: 0

Annexure-VI

One time Charges for Colocation & Managed Services

Description	Make	Model	UoM	Quantity (Q)	HSN Code	Unit Price in Rs.(P)	Total Pirce In Rs. (QxP)
Supply of 42 U, 600mm*1000mm Server Rack. (DC -10, DR-4)			Nos.	14			-
Powered On Colocation Full Rack space. 6 KVA Rated with Bundled Power. (DC)			Nos.	10			-
SS Cage with Biometric Access, CCTV Camera.			Lot	1			-
Powered On Colocation Full Rack space. 6 KVA Rated with Bundled Power. (DR)			Nos.	4			-
Copper Cross Connect Charges. Cat 6			Nos.	8			-
Seating Space in DC for OEM/ IP/ SI/ NMDC			Nos.	1			-
						Total	-

Note 1: Applicable taxe rates should be mentioned.
Note 2: All line items to be quoted. If any line item not indicated with price, the same will be considered as free of cost supply and PO placed accordingly.

Name of the supplier: 0
Mail Id: 0
Mobile: 0

Annexure-VI

NOC

Sr. No.	Network Components	Make	Model	Quantity (Q)	HSN Code	Unit Price in Rs.(P)	Total Pirce In Rs. (QxP)
1	Desktop for NOC			4			-
2	Console/Screen (LFD) for NOC room			2			-
3	Installation and Commissioning charges for the above			1			-
						Total	-

Note 1: **Applicable tax rates should be mentioned.**

Note 2: All line items to be quoted. If any line item not indicated with price, the same will be considered as free of cost supply and PO placed accordingly.

Name of the supplier: 0
Mail Id: 0
Mobile: 0

Annexure-VI

Recurring Item

	Price per year (A)	Price for 5 years (Ax5)
Colocation Services	Lumpsum	-
Managed Services	Lumpsum	-
Total		-

Note1 : Applicable taxe rates should be mentioned.
Note 2: All line items to be quoted. If any line item not indicated with price, the same will be considered as free of cost supply and PO placed accordingly.

Name of the supplier: 0
Mail Id: 0
Mobile: 0

ANNEXURE-VII

Consolidated PRICE BID:

S.No	Items	Total Price in Rs. (The Taxes/GST shall be extra)
1	DC/DR Hardware	-
2	DC/ DR Software	-
3	DC DR XMII SW & HW	-
4	Fire wall	-
5	Switch, EMS, etc..	-
6	Wi-Fi & Point to Point radio links	-
7	Campus Backbone Cabling	-
8	OFC Links @	-
9	One-time charges for Co-location and Managed Services	-
10	NOC	-
11	Co-Location & Managed Services for 5 years	-
	Total	-

Name of the supplier: 0
Mail Id: 0
Mobile: 0